



DOMESTIC ABUSE INTERVENTION PROGRAMS

202 East Superior Street
Duluth, Minnesota 55802
218-722-2781
www.theduluthmodel.org

Camila and James

Part I—Background Facts

Two weeks after Camila broke up with her boyfriend James and asked him to move out, she returns from work surprised to find him in her home. James tells Camila he is there to pick up his belongings. A neighbor overhears shouting and calls the police, but James is gone by the time the responding officer arrives. When the officer asks Camila what happened, she states that after she objected to James taking one of the items, he shoved her, grabbed her arm and began shouting obscenities. The officer notes that Camila’s upper arm was starting to bruise. When asked about James’ whereabouts, Camila states “I don’t know where he went but he said, ‘I’m going to ruin your life’ before leaving.” Camila also states that James has previously destroyed her property, followed her, and threatened her, but he never previously physically harmed hurt her or their daughter, who was currently with her grandmother. Camila also says that she is worried that she “will never get rid of him.”

Discussion:

- *What are some red flags that stand out about this incident?* (Examples: escalation of abuse, threats, destruction of property, stalking, history of violence, potential verbal abuse in front of the child.)
- *How serious is this behavior?*

Part II—Civil Court

Camila eventually decides to go to court and is granted an emergency order based on the above incident. After he’s served, James hires a private defense attorney. The attorney files for an order of protection against Camila, alleging that she began physically attacking James during the incident and he was merely trying to protect himself by holding her away. In the months prior to hearing, the defense attorney has sent nearly a dozen motions to Camila, mostly related to visitation and property. Outside the courtroom, Camila spots James talking to his attorney

in the hallway. She hovers around until they're looking away and hurries inside the courtroom before either of them see her. Camila checks in with the clerk, who informs her that her case will be at the end of the line. After some time, the judge finally calls her case.

Defense Attorney: Your honor, the victim has not responded to any of my client's motions. She's not allowing him to see their child, which my client is extremely worried about. He believes she is turning the child against him.

Judge: Would the petitioner like to respond?

Camila: Well, I told James he could see our child whenever he wants. But every time he calls me about visitation, he starts screaming at me, saying all sorts of names. I'm pretty sure I saw his car on my street last week, too.

Defense Attorney: Your honor, that's simply not true. The petitioner has no evidence of this. There's a temporary visitation schedule in place that she's required to follow. My client simply wants to see his kid regularly while the court sorts out the other issues. He has no interest in speaking with her otherwise.

Camila: Then why is he always messaging me and showing up to my house?

Judge: Ms. Costello, please wait until your turn to speak.

James: Your Honor, I just want to see my daughter. It's really painful being apart from her. And I'm trying to do anything I can to make this right for her.

Camila: You barely even show up on your weekends. And when you do, you just have your mother watch her while you're out with your friends!
(James' mother scoffs loudly in the back).

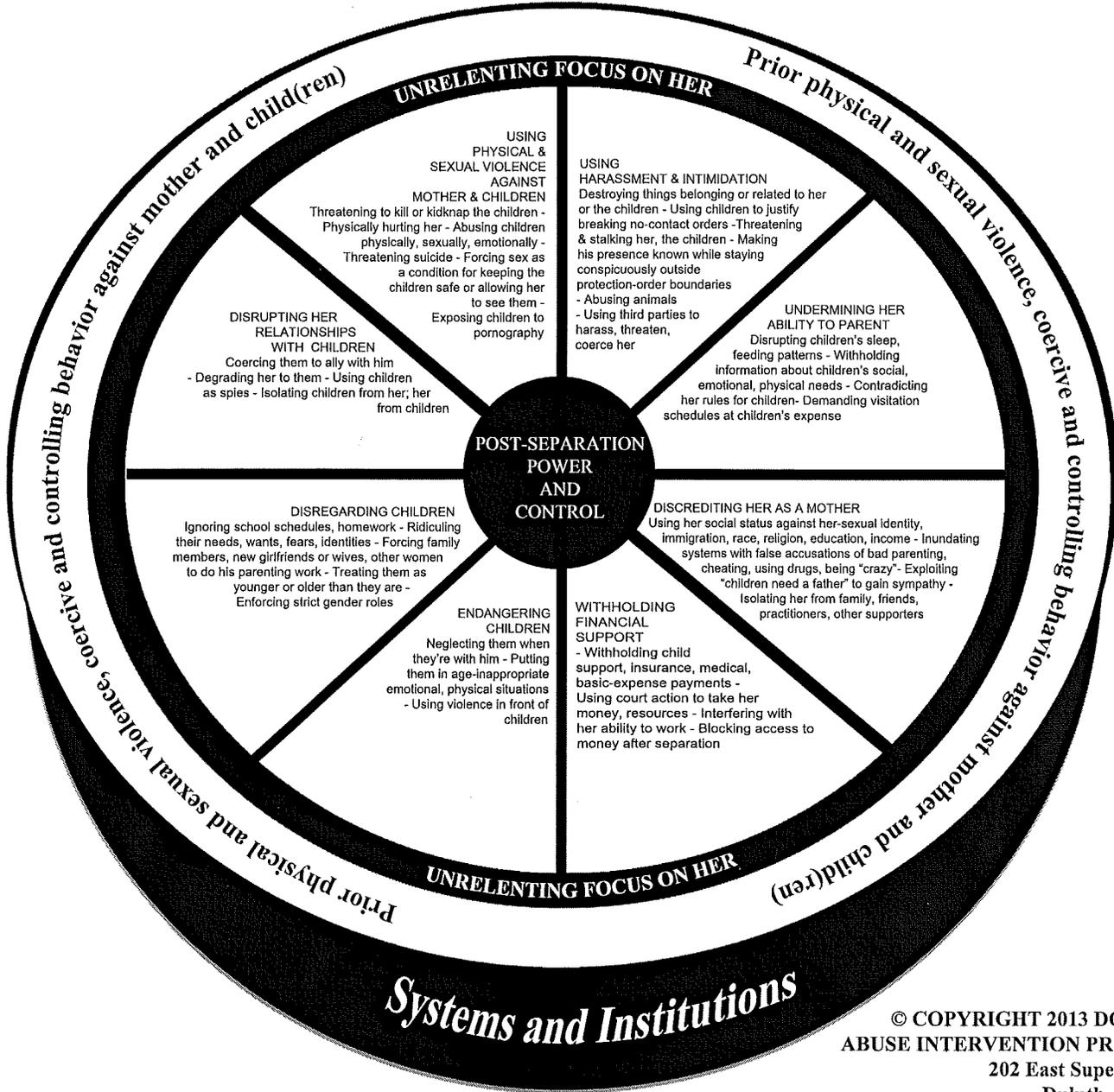
Judge: I don't want this back-and-forth in my courtroom. We're going to get supervised exchange to minimize any contact between the parties. No harassing phone calls and no preventing visitation. Do both parties understand?

Both Camila and James nod.

Discussion:

- *Do you often encounter this dynamic in the courthouse?*
- *What are the differences between Camila and James' behavior?*
- *How much of this information would you or your team know at the time of the hearing?*

Post Separation Power and Control Wheel



© COPYRIGHT 2013 DOMESTIC ABUSE INTERVENTION PROGRAMS
 202 East Superior Street
 Duluth, MN 55802
 218-722-2781
www.theduluthmodel.org

Section I: Inside and Around the Courthouse

Who in your court interacts with domestic violence-related litigants?	When and where do they have those interactions?	Where and how do those interactions overlap with others (<i>e.g.</i>, departments, services, etc.) inside the courthouse and within the community?

Section II: Beyond the Courthouse and Into the Community

Who in your community interacts with domestic violence-related litigants?	When and where do they have those interactions?	Where and how do those interactions overlap with others (e.g., departments, services, etc.) within the community and inside the courthouse?

States with Strangulation Legislation

This list was last updated by Grace Shuman at the Training Institute on Strangulation Prevention in March 2021. The list was originally created by the National District Attorneys Association and has subsequently been updated at various times with the help of Gael Strack, Casey Gwinn, Melissa Mack, Sarah Dawe, Sarah Sherman Julien, Fiona Wells, Elizabeth Cosentino-Vonderahe, and Katie Kirkwood. The Institute recommends checking both case law and current legislation for any updates or modifications.

States	TEXT
Alabama	<p>§ 13A-6-138. DOMESTIC VIOLENCE BY STRANGULATION OR SUFFOCATION. ENACTED AND/OR EFFECTED: 2012. UPDATED: 2019</p> <p>(a) For the purposes of this section, the following terms have the following meanings:</p> <p>1) STRANGULATION. Intentionally causing asphyxia by closure or compression of the blood vessels or air passages of the neck as a result of external pressure on the neck.</p> <p style="padding-left: 40px;">(2) SUFFOCATION. Intentionally causing asphyxia by depriving a person of air or by preventing a person from breathing through the inhalation of toxic gases or by blocking or obstructing the airway of a person, by any means other than by strangulation.</p> <p>(b) A person commits the crime of domestic violence by strangulation or suffocation if he or she commits an assault with intent to cause physical harm or commits the crime of menacing pursuant to Section 13A-6-23, by strangulation or suffocation or attempted strangulation or suffocation and the victim is a current or former spouse, parent, step-parent, child, step-child, any person with whom the defendant has a child in common, a present household member, or a person who has or had a dating relationship. For the purpose of this section, a household member excludes non-romantic or non-intimate co-residents, and a dating relationship means a current or former relationship of a romantic or intimate nature characterized by the expectation of affectionate or sexual involvement by either party.</p> <p>(c) Domestic violence by strangulation or suffocation is a Class B felony punishable as provided by law.</p>
Alaska	<p>ALASKA HB14. ASSAULT; SEX OFFENSES; SENT. AGGRAVATOR</p>

ENACTED AND/OR EFFECTED: 2009

UPDATED: 2019

* **Section 1.** AS 11.41.200(a) is amended to read:

(a) A person commits the crime of assault in the first-degree if

(1) that person recklessly causes serious physical injury to another by 8 means of a dangerous instrument;

(2) with intent to cause serious physical injury to another, the person 10 causes serious physical injury to any person;

(3) the person knowingly engages in conduct that results in serious physical injury to another under circumstances manifesting extreme indifference to the value of human life;
[OR]

(4) that person recklessly causes serious physical injury to another by repeated assaults using a dangerous instrument, even if each assault individually does 4 not cause serious physical injury; or

(5) that person knowingly causes another to become unconscious⁶ by means of a dangerous instrument; in this paragraph, "dangerous instrument" has the meaning given in AS 11.81.900(b)(15)(B).

* **Sec. 3.** AS 11.81.900(b)(15) is amended to read:

(15) "dangerous instrument" means

(A) any deadly weapon or anything that, under the circumstances in which it is used, attempted to be used, or threatened to be used, is capable of causing death or serious physical injury; or

(B) hands, other body parts, or other objects when used to impede normal breathing or circulation of blood by applying pressure on the throat or neck or obstructing the nose or mouth;

<p>Arizona</p>	<p style="text-align: center;">ARIZ. REV. STAT. § 13-1204. AGGRAVATED ASSAULT; CLASSIFICATION; DEFINITION ENACTED AND/OR EFFECTED: 2011</p> <p>(B) A person commits aggravated assault if the person commits assault by either intentionally, knowingly or recklessly causing any physical injury to another person, intentionally placing another person in reasonable apprehension of imminent physical injury or knowingly touching another person with the intent to injure the person, and both of the following occur:</p> <p>(1) The person intentionally or knowingly impedes the normal breathing or circulation of blood of another person by applying pressure to the throat or neck or by obstructing the nose and mouth either manually or through the use of an instrument.</p> <p>(2) Any of the circumstances exists that are set forth in section 13-3601, subsection A, paragraph 1, 2, 3, 4, 5 or 6.</p>
<p>Arkansas</p>	<p style="text-align: center;">ARK. CODE ANN. § 5-13-204. AGGRAVATED ASSAULT ENACTED AND/OR EFFECTED: 2009</p> <p>(a) A person commits aggravated assault if, under circumstances manifesting extreme indifference to the value of human life, he or she purposely:</p> <p>(3) Impedes or prevents the respiration of another person or the circulation of another person's blood by applying pressure on the throat or neck or by blocking the nose or mouth of the other person.</p> <p style="text-align: center;">Ark. Code § 12-18-103 ENACTED AND/OR EFFECTED: 2011</p> <p>Definitions (3) (A) "Abuse" means any of the following acts or omissions by a parent, guardian, custodian, foster parent, person eighteen (18) years of age or older living in the home with a child whether related or unrelated to the child, or any person who is entrusted with the child's care by a</p>

	<p>parent, guardian, custodian, or foster parent, including, but not limited to, an agent or employee of a public or private residential home, child care facility, public or private school, or any person legally responsible for the child's welfare, but excluding the spouse of a minor: *** (vii) Any of the following intentional or knowing acts, with or without physical injury: *** (c) Interfering with a child's breathing.</p>
--	--

<p>California</p>	<p align="center">CAL. PENAL CODE § 273.5. WILLFUL INFLICTION OF CORPORAL INJURY; VIOLATION; PUNISHMENT ENACTED AND/OR EFFECTED: 2011</p> <p>(a) Any person who willfully inflicts corporal injury resulting in a traumatic condition upon a victim described in subdivision (b) is guilty of a felony, and upon conviction thereof shall be punished by imprisonment in the state prison for two, three, or four years, or in a county jail for not more than one year, or by a fine of up to six thousand dollars (\$6,000) or by both that fine and imprisonment.</p> <p>(b) Subdivision (a) shall apply if the victim is or was one or more of the following: (1) The offender's spouse or former spouse. (2) The offender's cohabitant or former cohabitant. (3) The offender's fiancé or fiancée, or someone with whom the offender has, or previously had, an engagement or dating relationship, as defined in paragraph (10) of subdivision (f) of Section 243. (4) The mother or father of the offender's child.</p> <p>(c) Holding oneself out to be the husband or wife of the person with whom one is cohabiting is not necessary to constitute cohabitation as the term is used in this section.</p> <p>(d) As used in this section, "traumatic condition" means a condition of the body, such as a wound, or external or internal injury, including, but not limited to, injury as a result of strangulation or suffocation, whether of a minor or serious nature, caused by a physical force. For purposes of this section, "strangulation" and "suffocation" include impeding the normal breathing or circulation of the blood of a person by applying pressure on the throat or neck.</p> <p align="center">"Duty to Warn" ENACTED AND/OR EFFECTED: 2018</p> <p>A statement informing the victim that strangulation may cause internal injuries and encouraging the victim to seek medical attention.</p> <p align="center">CAL. PENAL CODE § 13730. RECORDING DOMESTIC VIOLENCE-RELATED CALLS; REPORTS</p> <p>a) Each law enforcement agency shall develop a system, by January 1, 1986, for recording all</p>
--------------------------	---

domestic violence-related calls for assistance made to the department, including whether weapons are involved, or whether the incident involved strangulation or suffocation. All domestic violence-related calls for assistance shall be supported with a written incident report, as described in subdivision (c), identifying the domestic violence incident. Monthly, the total number of domestic violence calls received and the numbers of those cases involving weapons or strangulation or suffocation shall be compiled by each law enforcement agency and submitted to the Attorney General.

(b) The Attorney General shall report annually to the Governor, the Legislature, and the public the total number of domestic violence-related calls received by California law enforcement agencies, the number of cases involving weapons, the number of cases involving strangulation or suffocation, and a breakdown of calls received by agency, city, and county.

(c) Each law enforcement agency shall develop an incident report form that includes a domestic violence identification code by January 1, 1986. In all incidents of domestic violence, a report shall be written and shall be identified on the face of the report as a domestic violence incident. The report shall include at least all of the following:

- (1) A notation of whether the officer or officers who responded to the domestic violence call observed any signs that the alleged abuser was under the influence of alcohol or a controlled substance.
- (2) A notation of whether the officer or officers who responded to the domestic violence call determined if any law enforcement agency had previously responded to a domestic violence call at the same address involving the same alleged abuser or victim.
- (3) A notation of whether the officer or officers who responded to the domestic violence call found it necessary, for the protection of the peace officer or other persons present, to inquire of the victim, the alleged abuser, or both, whether a firearm or other deadly weapon was present at the location, and, if there is an inquiry, whether that inquiry disclosed the presence of a firearm or other deadly weapon. Any firearm or other deadly weapon discovered by an officer at the scene of a domestic violence incident shall be subject to confiscation pursuant to Division 4 (commencing with Section 18250) of Title 2 of Part 6.
- (4) A notation of whether there were indications that the incident involved strangulation or suffocation. This includes whether any witness or victim reported any incident of strangulation or suffocation, whether any victim reported symptoms of strangulation or suffocation, or whether the officer observed any signs of strangulation or suffocation.

CA Civil Code § 43.92

Enacted to limit the liability of psychotherapists under Tarasoff regarding therapist's duty to warn an intended victim. When a therapist determines that his patient presents a serious danger of violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger. Thus, it may call for him to warn the intended victim or others likely to apprise the victim of the danger, to notify the police, or to take whatever other steps are reasonably necessary under the circumstances." (Tarasoff, supra, 17 Cal.3d at p. 431.)

CA. AB-3189 CONSENT BY MINORS TO TREATMENT FOR INTIMATE PARTNER VIOLENCE

ENACTED AND/OR EFFECTED: 2019

- (1) Existing law authorizes a minor who is 12 years of age or older and is alleged to have been raped, or a minor who is alleged to have been sexually assaulted, to consent to medical care related to the diagnosis and treatment of the condition and the collection of medical evidence with regard to the alleged rape or sexual assault. This bill would authorize a minor who is 12 years of age or older and who states he or she is injured as a result of intimate partner violence, as defined, to consent to medical care related to the diagnosis or treatment of the injury and the collection of medical evidence with regard to the alleged intimate partner violence. The bill would specify that this provision would not apply to a case in which a minor is an alleged victim of rape or is alleged to have been sexually assaulted, in which case the above-described provisions would apply.
- (2) Existing law requires a health practitioner who works in a certain type of health facility and provides medical services for a patient he or she knows or reasonably suspects is suffering from an injury caused by a firearm or assaultive or abusive conduct to make a report to a local law enforcement agency about the patient and the extent of the injuries.

This bill would require a health practitioner that believes a report is required pursuant to these provisions, when providing treatment to an above-described minor injured as a result of alleged intimate partner violence, to inform the minor that the report will be made and attempt to contact the minor's parent or guardian and inform him or her of the report, except as specified.

<p>Colorado</p>	<p>Colorado Criminal Code § 18-3-203. Offenses Against the Person; Assault in the second degree ENACTED AND/OR EFFECTED: 2016</p> <ul style="list-style-type: none"> • A person commits the crime of assault in the first degree if: <ul style="list-style-type: none"> ▫ With the intent to cause serious bodily injury ▫ s/he applies sufficient pressure to Impede or restrict the breathing or circulation of blood of another person ▫ By applying such pressure to the neck or by blocking the nose or mouth of the other person and ▫ Thereby causes serious injury <p style="text-align: center;">CRS § 18-1-901. Definition of Serious Bodily Injury</p> <p>Bodily injury which, either at the time of the actual injury or at a later time involves:</p> <ul style="list-style-type: none"> ▫ A substantial risk of death ▫ A substantial risk of serious permanent disfigurement ▫ A substantial risk of protracted loss or impairment of the function of any part or organ of the body ▫ Breaks, fractures or burns of the second or third degree
<p>Connecticut</p>	<p>Conn. Gen. Stat. § 53a-64aa. Strangulation in the first degree: Class C felony ENACTED AND/OR EFFECTED: 2007</p> <p>(a) A person is guilty of strangulation in the first degree when such person commits strangulation in the second degree as provided in section 53a-64bb and (1) in the commission of such offense, such person (A) uses or attempts to use a dangerous instrument, or (B) causes serious physical injury to such other person, or (2) such person has previously been convicted of a violation of this section or section 53a-64bb.</p> <p>(b) No person shall be found guilty of strangulation in the first degree and unlawful restraint or assault upon the same incident, but such person may be charged and prosecuted for all three offenses upon the same information. For the purposes of this section, "unlawful restraint" means a violation of section 53a-95 or 53a-96, and "assault" means a violation of section 53a-59, 53a-59a,</p>

53a-59b, 53a-59c, 53a-60, 53a-60a, 53a-60b, 53a-60c, 53a-61 or 53a-61a.

(c) Strangulation in the first degree is a class C felony.

§ 53a-64bb. Strangulation in the second degree: Class D felony

(a) A person is guilty of strangulation in the second degree when such person restrains another person by the neck or throat with the intent to impede the ability of such other person to breathe or restrict blood circulation of such other person and such person impedes the ability of such other person to breathe or restricts blood circulation of such other person.

(b) No person shall be found guilty of strangulation in the second degree and unlawful restraint or assault upon the same incident, but such person may be charged and prosecuted for all three offenses upon the same information. For the purposes of this section, "unlawful restraint" means a violation of section 53a-95 or 53a-96, and "assault" means a violation of section 53a-59, 53a-59a, 53a-59b, 53a-59c, 53a-60, 53a-60a, 53a-60b, 53a-60c, 53a-61 or 53a-61a.

(c) Strangulation in the second degree is a class D felony.

Conn. Gen. Stat. § 53a-64cc. Strangulation in the third degree: Class A misdemeanor

(a) A person is guilty of strangulation in the third degree when such person recklessly restrains another person by the neck or throat and impedes the ability of such other person to breathe or restricts blood circulation of such other person.

(b) No person shall be found guilty of strangulation in the third degree and unlawful restraint or assault upon the same incident, but such person may be charged and prosecuted for all three offenses upon the same information. For the purposes of this section, "unlawful restraint" means a violation of section 53a-95 or 53a-96, and "assault" means a violation of section 53a-59, 53a-59a, 53a-59b, 53a-59c, 53a-60, 53a-60a, 53a-60b, 53a-60c, 53a-61 or 53a-61a.

(c) Strangulation in the third degree is a class A misdemeanor.

<p>Delaware</p>	<p style="text-align: center;">11 Del. C. § 607. Strangulation; penalty; affirmative defense ENACTED AND/OR EFFECTED: 2010</p> <p>(a)(1) A person commits the offense of strangulation if the person knowingly or intentionally impedes the breathing or circulation of the blood of another person by applying pressure on the throat or neck of the other person.</p> <p>(2) Except as provided in paragraph (a)(3) of this section, strangulation is a class E felony.</p> <p>(3) Strangulation is a class D felony if:</p> <ul style="list-style-type: none"> a. The person used or attempted to use a dangerous instrument or a deadly weapon while committing the offense; or b. The person caused serious physical injury to the other person while committing the offense; or c. The person has been previously convicted of strangulation. <p>(b) It is an affirmative defense that an act constituting strangulation was the result of a legitimate medical procedure.</p>
<p>Florida</p>	<p style="text-align: center;">FLA. STAT. ANN. § 784.041 FELONY BATTERY; DOMESTIC BATTERY BY STRANGULATION ENACTED AND/OR EFFECTED: 2007</p> <p>(1) A person commits felony battery if he or she:</p> <ul style="list-style-type: none"> (a) Actually and intentionally touches or strikes another person against the will of the other; and (b) Causes great bodily harm, permanent disability, or permanent disfigurement. <p>(2) (a) A person commits domestic battery by strangulation if the person knowingly and intentionally, against the will of another, impedes the normal breathing or circulation of the blood of a family or household member or of a person with whom he or she is in a dating relationship, so as to create a risk of or cause great bodily harm by applying pressure on the throat or neck of the other person or by blocking the nose or mouth of the other person. This paragraph does not apply to any act of medical diagnosis, treatment, or prescription which is authorized under the laws of this state.</p>

	<p>(b) As used in this subsection, the term:</p> <ol style="list-style-type: none">1. "Family or household member" has the same meaning as in s. 741.28.2. "Dating relationship" means a continuing and significant relationship of a romantic or intimate nature. <p>(3) A person who commits felony battery or domestic battery by strangulation commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.</p>
--	--

<p>Georgia</p>	<p style="text-align: center;">GA. CODE ANN., § 16-5-21 AGGRAVATED ASSAULT ENACTED AND/OR EFFECTED: 2014</p> <p>(a) As used in this Code section, the term “strangulation” means impeding the normal breathing or circulation of blood of another person by applying pressure to the throat or neck of such person or by obstructing the nose and mouth of such person.</p> <p>(b) A person commits the offense of aggravated assault when he or she assaults:</p> <p>(1) With intent to murder, to rape, or to rob;</p> <p>(2) With a deadly weapon or with any object, device, or instrument which, when used offensively against a person, is likely to or actually does result in serious bodily injury;</p> <p>(3) With any object, device, or instrument which, when used offensively against a person, is likely to or actually does result in strangulation; or</p> <p>(4) A person or persons without legal justification by discharging a firearm from within a motor vehicle toward a person or persons.</p>
<p>Hawaii</p>	<p style="text-align: center;">HAW. REV. STAT. § 709-906(1), (8) ABUSE OF FAMILY OR HOUSEHOLD MEMBERS; PENALTY ENACTED AND/OR EFFECTED: 2006. Amended: 2019</p> <p>(1) It shall be unlawful for any person, singly or in concert, to physically abuse a family or household member or to refuse compliance with the lawful order of a police officer under subsection (4). The police, in investigating any complaint of abuse of a family or household member, upon request, may transport the abused person to a hospital or safe shelter.</p> <p>For the purposes of this section, "family or household member" means spouses or reciprocal beneficiaries, former spouses or reciprocal beneficiaries, persons who have a child in common, parents, children, persons related by consanguinity, and persons jointly residing or formerly residing in the same dwelling unit.</p> <p>(8) Where the physical abuse consists of intentionally or knowingly causing bodily injury by impeding normal breathing or circulation of the blood by:</p> <p style="margin-left: 40px;">a. Applying Pressure on the throat or the neck with any part of the body or ligature;</p> <p style="margin-left: 40px;">b. Blocking the nose and mouth; or</p> <p style="margin-left: 40px;">c. Applying pressure to the chest,</p> <p>abuse of a family or household member is a class C felony; provided that infliction of visible bodily</p>

	injury shall not be required to establish an offense under this subsection.
--	---

<p>Idaho</p>	<p style="text-align: center;">IDAHO CODE ANN. § 18-923. ATTEMPTED STRANGULATION EFFECTIVE: 2005, AMENDED: 2018</p> <p>(1) Any person who willfully and unlawfully chokes or attempts to strangle a household member, or a person with whom he or she has or had a dating relationship, is guilty of a felony punishable by incarceration for up to fifteen (15) years in the state prison.</p> <p>(2) No injuries are required to prove attempted strangulation.</p> <p>(3) The prosecution is not required to show that the defendant intended to kill or injure the victim. The only intent required is the intent to choke or attempt to strangle.</p> <p>(4) "Household member" assumes the same definition as set forth in section 18-918(1)(a), Idaho Code.</p> <p>(5) "Dating relationship" assumes the same definition as set forth in section 39-6303(2), Idaho Code.</p> <p>(2) (a) Any household member who in committing a battery, as defined in section 18-903, Idaho Code, inflicts a traumatic injury upon any other household member is guilty of a felony. (b) A conviction of felony domestic battery is punishable by imprisonment in the state prison for a term not to exceed ten (10) years or by a fine not to exceed ten thousand dollars (\$10,000) or by both fine and imprisonment.</p> <p style="text-align: center;">H.B. 360</p> <p>Amends existing law relating to assault and battery; revises a provision relating to counseling; provides that the Supreme Court shall establish a certain rule; provides that a person guilty of attempted strangulation shall undergo a certain evaluation, counseling, and other treatment.</p>
<p>Illinois</p>	<p style="text-align: center;">ILL. COMP. STAT. ANN. 5/ § 12-3.05. Aggravated battery. ENACTED AND/OR EFFECTED: 2010</p>

	<p>(a) Offense based on injury. A person commits aggravated battery when, in committing a battery, other than by the discharge of a firearm, he or she knowingly does any of the following: (5) Strangles another individual.</p> <p>“Strangle” means intentionally impeding the normal breathing or circulation of the blood of an individual by applying pressure on the throat or neck of that individual or by blocking the nose or mouth of that individual.</p> <p>(h) Sentence. Unless otherwise provided, aggravated battery is a Class 3 felony. Aggravated battery under subdivision (a)(5) is a Class 1 felony if: (A) the person used or attempted to use a dangerous instrument while committing the offense; or (B) the person caused great bodily harm or permanent disability or disfigurement to the other person while committing the offense; or (C) the person has been previously convicted of a violation of subdivision (a)(5) under the laws of this State or laws similar to subdivision (a)(5) of any other state.</p> <p>ILCS 725. Criminal Procedure § 5/110-5. Determining the amount of bail and conditions of release ENACTED AND/OR EFFECTED: 2017</p> <p>F) When a person is charged with a violation of an order of protection under Section 12-3.4 or 12-30 of the Criminal Code of 1961 or the Criminal Code of 2012 or when a person is charged with domestic battery, aggravated domestic battery, kidnapping, aggravated kidnaping, unlawful restraint, aggravated unlawful restraint, stalking, aggravated stalking, cyberstalking, harassment by telephone, harassment through electronic communications, or an attempt to commit first degree murder committed against an intimate partner regardless whether an order of protection has been issued against the person,</p> <ul style="list-style-type: none">(1) whether the alleged incident involved harassment or abuse, as defined in the Illinois Domestic Violence Act of 1986;(2) whether the person has a history of domestic violence, as defined in the Illinois Domestic Violence Act, or a history of other criminal acts;(3) based on the mental health of the person;(4) whether the person has a history of violating the orders of any court or governmental entity;
--	--

	<p>(5) whether the person has been, or is, potentially a threat to any other person;</p> <p>(6) whether the person has access to deadly weapons or a history of using deadly weapons;</p> <p>(7) whether the person has a history of abusing alcohol or any controlled substance;</p> <p>(8) based on the severity of the alleged incident that is the basis of the alleged offense, including, but not limited to, the duration of the current incident, and whether the alleged incident involved the use of a weapon, physical injury, sexual assault, strangulation, abuse during the alleged victim's pregnancy, abuse of pets, or forcible entry to gain access to the alleged victim;</p> <p>(9) whether a separation of the person from the alleged victim or a termination of the relationship between the person and the alleged victim has recently occurred or is pending;</p> <p>(10) whether the person has exhibited obsessive or controlling behaviors toward the alleged victim, including, but not limited to, stalking, surveillance, or isolation of the alleged victim or victim's family member or members;</p> <p>(11) whether the person has expressed suicidal or homicidal ideations;</p> <p>(12) based on any information contained in the complaint and any police reports, affidavits, or other documents accompanying the complaint, the court may, in its discretion, order the respondent to undergo a risk assessment evaluation using a recognized, evidence-based instrument conducted by an Illinois Department of Human Services approved partner abuse intervention program provider, pretrial service, probation, or parole agency. These agencies shall have access to summaries of the defendant's criminal history, which shall not include victim interviews or information, for the risk evaluation. Based on the information collected from the 12 points to be considered at a bail hearing under this subsection (f), the results of any risk evaluation conducted and the other circumstances of the violation, the court may order that the person, as a condition of bail, be placed under electronic surveillance as provided in Section 5-8A-7 of the Unified Code of Corrections.</p>
--	--

<p>Indiana</p>	<p style="text-align: center;">IND. CODE ANN. § 35-42-2-9. STRANGULATION ENACTED AND/OR EFFECTED: 2006</p> <p>(a) This section does not apply to a medical procedure.</p> <p>(b) As used in this section, “torso” means any part of the upper body from the collarbone to the hips</p> <p>(c) A person who, in a rude, angry, or insolent manner, knowingly or intentionally:</p> <p style="padding-left: 40px;">(1) applies pressure to the throat or neck of another person; or</p> <p style="padding-left: 40px;">(2) obstructs the nose or mouth of another person;</p> <p>in a manner that impedes the normal breathing or the blood circulation of the other person commits strangulation, a level 6 felony.</p> <p>(d) However, the offense under subsection (c) is a Level 5 felony if:</p> <p style="padding-left: 40px;">(1) the offense is committed against a pregnant woman; and</p> <p style="padding-left: 40px;">(2) the person who committed the offense knew the victim was pregnant at the time of the offense.</p> <p style="text-align: center;">Ind. Marion Cir. & Superior Crim. Rule 108 – Bail Enhancements ENACTED AND/OR EFFECTED: 2017</p> <p>B. Enhancements- The bail schedule amounts shall double, up to a maximum of \$5,000 for each of the following circumstances:</p> <p style="padding-left: 40px;">4. The defendant is charged with a Class D felony including strangulation</p>
<p>Iowa</p>	<p style="text-align: center;">I.C.S. § 708.2A (22, 1) DOMESTIC ABUSE ASSAULT — MANDATORY MINIMUMS, PENALTIES ENHANCED — EXTENSION OF NO-CONTACT ORDER ENACTED AND/OR EFFECTED: 2012</p> <p>1. For the purposes of this chapter, “domestic abuse assault” means an assault, as defined in section 708.1, which is domestic abuse as defined in section 236.2, subsection 2, paragraph “a”, “b”, “c”, or “d”.</p> <p>2. On a first offense of domestic abuse assault, the person commits:</p> <p style="padding-left: 40px;">d. An aggravated misdemeanor, if the domestic abuse assault is committed by knowingly impeding the normal breathing or circulation of the blood of another by applying pressure to the throat or neck of the other person or by obstructing the nose or mouth of the other person.</p> <p>3. Except as otherwise provided in subsection 2, on a second domestic abuse assault, a person</p>

	<p>commits:</p> <ul style="list-style-type: none">a. A serious misdemeanor, if the first offense was classified as a simple misdemeanor, and the second offense would otherwise be classified as a simple misdemeanor.b. An aggravated misdemeanor, if the first offense was classified as a simple or aggravated misdemeanor, and the second offense would otherwise be classified as a serious misdemeanor, or the first offense was classified as a serious or aggravated misdemeanor, and the second offense would otherwise be classified as a simple or serious misdemeanor. <p>4. On a third or subsequent offense of domestic abuse assault, a person commits a class “D” felony.</p> <p>5. For a domestic abuse assault committed by knowingly impeding the normal breathing or circulation of the blood of another by applying pressure to the throat or neck of the other person or by obstructing the nose or mouth of the other person, and causing bodily injury, the person commits a class “D” felony.</p>
--	--

<p>Kansas</p>	<p style="text-align: center;">KS § 21-5414; Aggravated Domestic Battery ENACTED AND/OR EFFECTED: 2017</p> <p>Aggravated domestic battery is:</p> <ul style="list-style-type: none"> • (1) Knowingly impeding the normal breathing or circulation of the blood by applying pressure on the throat, neck or chest of a person with whom the offender is involved or has been involved in a dating relationship or a family or household member, when done in a rude, insulting or angry manner; or (2) knowingly impeding the normal breathing or circulation of the blood by blocking the nose or mouth of a person with whom the offender is involved or has been involved in a dating relationship or a family or household member, when done in a rude, insulting or angry manner.” • Aggravated domestic battery is a severity level 7, person felony. • (d) In determining the sentence to be imposed within the limits provided for a first, second, third or subsequent offense under this section, a court shall consider information presented to the court relating to any current or prior protective order issued against such person.
<p>Kentucky</p>	<p style="text-align: center;">KY REV. STAT. § 508</p> <p style="text-align: center;">SECTION 1</p> <p>(1) A person is guilty of strangulation in the first degree when the person, without consent, intentionally impedes the normal breathing or circulation of the blood of another person by: (a) Applying pressure on the throat or neck of the other person; or (b) Blocking the nose or mouth of the other person.</p> <p>(2) Strangulation in the first degree is a Class C felony.</p> <p style="text-align: center;">SECTION 2</p> <p>(1) A person is guilty of strangulation in the second degree when the person, without consent, wantonly impedes the normal breathing or circulation of the blood of another person by: (a) Applying pressure on the throat or neck of the other person; or (b) Blocking the nose or mouth of the other person.</p> <p>(2) Strangulation in the second degree is a Class D felony.</p>

	<p style="text-align: center;">SECTION 3</p> <p>KRS 403.720 is amended to read as follows:</p> <p>As used in KRS 403.715 to 403.785: (1) “Domestic violence and abuse” means physical injury, serious physical injury, stalking, sexual abuse, strangulation, assault, or the infliction of fear of imminent physical injury, serious physical injury, sexual abuse, strangulation, or assault between family members or members of an unmarried couple</p>
--	--

<p>Louisiana</p>	<p style="text-align: center;">LA. REV. STAT. ANN. § 14:35.3(B)(3). DOMESTIC ABUSE BATTERY ENACTED AND/OR EFFECTED: 2006</p> <p>A. Domestic abuse battery is the intentional use of force or violence committed by one household member upon the person of another household member.</p> <p>B. For purposes of this Section:</p> <p>(3) "Household member" means any person of the opposite sex presently living in the same residence or living in the same residence within five years of the occurrence of the domestic abuse battery with the defendant as a spouse, whether married or not, or any child presently living in the same residence or living in the same residence within five years immediately prior to the occurrence of domestic abuse battery, or any child of the offender regardless of where the child resides.</p> <p>(4) "Serious bodily injury" means bodily injury that involves unconsciousness, extreme physical pain, or protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty, or a substantial risk of death.</p> <p>(5) "Strangulation" means intentionally impeding the normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of the victim.</p> <p style="text-align: center;">LA. REV. STAT. §2. DEFINITIONS</p> <p>...</p> <p>B. In this Code, "crime of violence" means an offense that has, as an element, the use, attempted use, or threatened use of physical force against the person or property of another, and that, by its very nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense or an offense that involves the possession or use of a dangerous weapon. The following enumerated offenses and attempts to commit any of them are included as "crimes of violence":</p> <p>... (45) Domestic abuse aggravated assault.</p> <p>... (47) Aggravated assault upon a dating partner.</p>
-------------------------	---

(48) Domestic abuse battery punishable under R.S. 14:35.3(L), (M)(2), (N), (O), or (P).

(49) Battery of a dating partner punishable under R.S. 14:34.9(L), (M)(2), (N), (O), or (P).

LA Code Crim. Pro 330.3 - Bail hearing for certain offenses against a family or household member or dating partner

ENACTED AND/OR EFFECTED: 2015

A. This Article may be cited as and referred to as "Gwen's Law".

B. A contradictory bail hearing, as provided for in this Article, may be held prior to setting bail for a person in custody who is charged with domestic abuse battery, violation of protective orders, stalking, or any felony offense involving the use or threatened use of force or a deadly weapon upon the defendant's family member, as defined in R.S. 46:2132 or upon the defendant's household member as defined in R.S. 14:35.3, or upon the defendant's dating partner, as defined in R.S. 46:2151. If the court orders a contradictory hearing, the hearing shall be held within five days from the date of determination of probable cause, exclusive of weekends and legal holidays. At the contradictory hearing, the court shall determine the conditions of bail or whether the defendant should be held without bail pending trial. If the court decides not to hold a contradictory hearing, it shall notify the prosecuting attorney prior to setting bail.

C. In addition to the factors listed in Article 334, in determining whether the defendant should be admitted to bail pending trial, or in determining the conditions of bail, the judge or magistrate shall consider the following:

(1) The criminal history of the defendant.

(2) The potential threat or danger the defendant poses to the victim, the family of the victim, or to any member of the public, especially children.

(3) Documented history or records of any of the following: substance abuse by the defendant; threats of suicide by the defendant; the defendant's use of force or threats of use of force against any victim; **strangulation**, forced sex, or controlling the activities of any victim by the defendant; or threats to kill. Documented history or records may include but are not limited to sworn affidavits, police reports, and medical records.

D. Following the contradictory hearing and based upon the judge's or magistrate's review of

	<p>the factors set forth in Paragraph C of this Article, the judge or magistrate may order that the defendant not be admitted to bail, upon proof by clear and convincing evidence either that the defendant might flee, or that the defendant poses an imminent danger to any other person or the community.</p>
--	---

<p>Maine</p>	<p style="text-align: center;">17- AM.R.S.A. § 208. AGGRAVATED ASSAULT. ENACTED AND/OR EFFECTED: 2012. UPDATED: 2019</p> <p>1. A person is guilty of aggravated assault if that person intentionally, knowingly or recklessly causes:</p> <ul style="list-style-type: none">A. Bodily injury to another that creates a substantial risk of death or extended convalescence necessary for recovery of physical health. Violation of this paragraph is a Class B crime;A-1. Bodily injury to another that causes serious, permanent disfigurement or loss or substantial impairment of the function of any bodily member or organ. Violation of this paragraph is a Class A crime;B. Bodily injury to another with use of a dangerous weapon. Violation of this paragraph is a Class B crime; orC. Bodily injury to another under circumstances manifesting extreme indifference to the value of human life. Such circumstances include, but are not limited to, the number, location or nature of the injuries, the manner or method inflicted, the observable physical condition of the victim or the use of strangulation. For the purpose of this paragraph, “strangulation” means impeding the breathing or circulation of the blood of another person by intentionally, knowingly or recklessly applying pressure on the person's throat or neck. Violation of this paragraph is a Class B crime. <p style="text-align: center;">LD 1027: An Act to Make Strangulation an Aggravating Sentencing Factor ENACTED AND/OR EFFECTED: 2011</p> <p>Emergency preamble. Whereas, acts and resolves of the Legislature do not become effective until 90 days after adjournment unless enacted as emergencies; and Whereas, there is a national increased awareness of the severity of strangulation, including its high prevalence in domestic and sexual assaults, its serious impacts, including life-threatening levels of anoxic brain damage, and its use as a tool of intimidation; and Whereas, public and professional awareness of the prevalence and impact of strangulation in Maine may lag behind research data; and Whereas, stakeholders should promptly review best practices models and tailor them to fit Maine's needs; and Whereas, in the judgment of the Legislature, these facts create an emergency within the meaning of the Constitution of Maine and require the following legislation as immediately necessary for the preservation of the public peace, health and safety; now, therefore, be it</p>
---------------------	--

<p>Maryland</p>	<p style="text-align: center;">ALL ENACTED AND/OR EFFECTED: 2007</p> <p style="text-align: center;">Md. CODE ANN., [CRIM. LAW] § 3-303(A). RAPE IN THE FIRST DEGREE</p> <p>(a) Prohibited. -- A person may not:</p> <ul style="list-style-type: none">(1) engage in vaginal intercourse with another by force, or the threat of force, without the consent of the other; and(2) (i) employ or display a dangerous weapon, or a physical object that the victim reasonably believes is a dangerous weapon;<li style="padding-left: 2em;">(ii) suffocate, <u>strangle</u>, disfigure, or inflict serious physical injury on the victim or another in the course of committing the crime;<li style="padding-left: 2em;">(iii) threaten, or place the victim in fear, that the victim, or an individual known to the victim, imminently will be subject to death, suffocation, strangulation, disfigurement, serious physical injury, or kidnapping;<li style="padding-left: 2em;">(iv) commit the crime while aided and abetted by another; or<li style="padding-left: 2em;">(v) commit the crime in connection with a burglary in the first, second, or third degree. <p style="text-align: center;">Md. CODE ANN., [CRIM. LAW] § 3-305(A). SEXUAL OFFENSE IN THE FIRST DEGREE</p> <p>(a) Prohibited. -- A person may not:</p> <ul style="list-style-type: none">(1) engage in a sexual act with another by force, or the threat of force, without the consent of the other; and(2) (i) employ or display a dangerous weapon, or a physical object that the victim reasonably believes is a dangerous weapon;<li style="padding-left: 2em;">(ii) suffocate, strangle, disfigure, or inflict serious physical injury on the victim or another in the course of committing the crime;<li style="padding-left: 2em;">(iii) threaten, or place the victim in fear, that the victim, or an individual known to the victim,
------------------------	---

<p>Maryland (cont.)</p>	<p>imminently will be subject to death, suffocation, strangulation, disfigurement, serious physical injury, or kidnapping;</p> <p>(iv) commit the crime while aided and abetted by another; or</p> <p>(v) commit the crime in connection with a burglary in the first, second, or third degree</p> <p>MD. CODE ANN., [CRIM. LAW] § 3-307(A)(1). SEXUAL OFFENSE IN THE THIRD DEGREE</p> <p>(a) Prohibited. -- A person may not:</p> <p>(1) (i) engage in sexual contact with another without the consent of the other; and</p> <p>(ii) 1. employ or display a dangerous weapon, or a physical object that the victim reasonably believes is a dangerous weapon;</p> <p>2. suffocate, strangle, disfigure, or inflict serious physical injury on the victim or another in the course of committing the crime;</p> <p>3. threaten, or place the victim in fear, that the victim, or an individual known to the victim, imminently will be subject to death, suffocation, strangulation, disfigurement, serious physical injury, or kidnapping;</p>
------------------------------------	--

<p>Massachusetts</p>	<p style="text-align: center;">Mass. Gen. Laws Ann. 265, § 15D ENACTED AND/OR EFFECTED: 2014</p> <p>SECTION 24. Said chapter 265 is hereby further amended by inserting after section 15C the following Section 15D.</p> <p>(a) For the purposes of this section the following words shall have the following meanings, unless the context clearly indicates otherwise:</p> <p style="padding-left: 40px;">"Serious bodily injury", bodily injury that results in a permanent disfigurement, loss or impairment of a bodily function, limb or organ or creates a substantial risk of death.</p> <p style="padding-left: 40px;">"Strangulation", the intentional interference of the normal breathing or circulation of blood by applying substantial pressure on the throat or neck of another.</p> <p style="padding-left: 40px;">"Suffocation", the intentional interference of the normal breathing or circulation of blood by blocking the nose or mouth of another.</p> <p>(b) Whoever strangles or suffocates another person shall be punished by imprisonment in state prison for not more than 5 years or in the house of correction for not more than 2 ½ years, or by a fine of not more than \$5,000, or by both such fine and imprisonment.</p> <p>(c) Whoever:</p> <ul style="list-style-type: none">(i) strangles or suffocates another person and by such strangulation or suffocation causes serious bodily injury;(ii) strangles or suffocates another person, who is pregnant at the time of such strangulation or suffocation, knowing or having reason to know that the person is pregnant;(iii) is convicted of strangling or suffocating another person after having been previously convicted of the crime of strangling or suffocating another person under this section, or of a like offense in another state or the United States or a military, territorial or Indian tribal authority; or(iv) strangles or suffocates another person, with knowledge that the individual has an outstanding temporary or permanent vacate, restraining or no contact order or judgment issued under sections 18 or 34B of chapter 208, section 32 of chapter 209, sections 3, 4 or 5
-----------------------------	---

	<p>of chapter 209A or sections 15 or 20 of chapter 209C , in effect against such person at the time the offense is committed, shall be punished by imprisonment in state prison for not more than 10 years, or in the house of correction for not more than 2½ years, and by a fine of not more than \$10,000.</p> <p>(d) For any violation of this section, or as a condition of a continuance without a finding, the court shall order the defendant to complete a certified batterer’s intervention program unless, upon good cause shown, the court issues specific written findings describing the reasons that batterer’s intervention should not be ordered or unless the batterer’s intervention program determines that the defendant is not suitable for intervention.</p> <p>***** Additional Legislation Requirements Pursuant to MA Legis 260</p> <ul style="list-style-type: none">• Basic Police Training Curriculum must include documentation, report writing and evidence collection, including gathering information on whether there have been specific instances of strangulation or suffocation of the victim by the suspect (Chapter 6 Section 116A(b)(11)(ix)• District Attorneys’ Offices must provide training to district attorneys, including gathering information on whether there have been specific instances of strangulation or suffocation of the victim by the suspect (Chapter 12 section 33(3)(ix)• The courts must provide training to judges, clerks, probation officers, court officers, security officers, and guardians ad litem, including gathering information on whether there have been specific instances of strangulation or suffocation of the victim by the suspect (Chapter 211B section 9B(3)(ix)
--	---

<p>Michigan</p>	<p>M.C.L.A. 750.84 - Assault with intent to do great bodily harm less than murder; assault by strangulation or suffocation ENACTED AND/OR EFFECTED: 2013</p> <p>Sec. 84. (1) A person who does either of the following is guilty of a felony punishable by imprisonment for not more than 10 years or a fine of not more than \$5,000.00, or both:</p> <p>(a) Assaults another person with intent to do great bodily harm, less than the crime of murder.</p> <p>(b) Assaults another person by strangulation or suffocation.</p> <p>(2) As used in this section, "strangulation or suffocation" means intentionally impeding normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person.</p> <p>(3) This section does not prohibit a person from being charged with, convicted of, or punished for any other violation of law arising out of the same conduct as the violation of this section.</p>
<p>Minnesota</p>	<p>MINN. STAT. § 609.2247. DOMESTIC ASSAULT BY STRANGULATION ENACTED AND/OR EFFECTED: 2005</p> <p>Subdivision 1. Definitions. (a) As used in this section, the following terms have the meanings given.</p> <p>(c) "Strangulation" means intentionally impeding normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person.</p> <p>Subd. 2. Crime. Unless a greater penalty is provided elsewhere, whoever assaults a family or household member by strangulation is guilty of a felony and may be sentenced to imprisonment for not more than three years or to payment of a fine of not more than \$5,000, or both.</p>

<p>Mississippi</p>	<p>MISS. CODE ANN. § 97-3-7. SIMPLE AND AGGRAVATED ASSAULT; SIMPLE AND AGGRAVATED DOMESTIC VIOLENCE ENACTED AND/OR EFFECTED: 2010</p> <p>(4)(a) When the offense is committed against a current or former spouse of the defendant or a child of that person, a person living as a spouse or who formerly lived as a spouse with the defendant or a child of that person, a parent, grandparent, child, grandchild or someone similarly situated to the defendant, a person who has a current or former dating relationship with the defendant, or a person with whom the defendant has had a biological or legally adopted child, a person is guilty of aggravated domestic violence who:</p> <ul style="list-style-type: none"> (i) Attempts to cause serious bodily injury to another, or causes such an injury purposely, knowingly or recklessly under circumstances manifesting extreme indifference to the value of human life; (ii) Attempts to cause or purposely or knowingly causes bodily injury to another with a deadly weapon or other means likely to produce death or serious bodily harm; or (iii) Strangles, or attempts to strangle another. <p>Upon conviction, the defendant shall be punished by imprisonment in the custody of the Department of Corrections for not less than two (2) nor more than twenty (20) years.</p> <p>(b) Aggravated domestic violence; third. A person is guilty of aggravated domestic violence third who, at the time of the commission of that offense, commits aggravated domestic violence as defined in this subsection (4) and who has two (2) prior convictions within the past seven (7) years, whether against the same or another victim, for any combination of aggravated domestic violence under this subsection (4) or simple domestic violence third as defined in subsection (3) of this section, or substantially similar offenses under the laws of another state, of the United States, or of a federally recognized Native American tribe. Upon conviction for aggravated domestic violence third, the defendant shall be sentenced to a term of imprisonment of not less than ten (10) nor more than twenty (20) years.</p> <p>(5) Sentencing for fourth or subsequent domestic violence offense. Any person who commits an offense defined in subsection (3) or (4) of this section, and who, at the time of the commission of that offense, has at least three (3) previous convictions, whether against the same or different victims, for any combination of offenses defined in subsections (3) and (4) of this section or substantially similar offenses under the law of another state, of the United States, or of a federally</p>
---------------------------	--

	<p>recognized Native American tribe, shall, upon conviction, be sentenced to imprisonment for not less than fifteen (15) years nor more than twenty (20) years.</p> <p>(6) In sentencing under subsections (3), (4) and (5) of this section, the court shall consider as an aggravating factor whether the crime was committed in the physical presence or hearing of a child under sixteen (16) years of age who was, at the time of the offense, living within either the residence of the victim, the residence of the perpetrator, or the residence where the offense occurred.</p> <p>(a) "Strangle" means to restrict the flow of oxygen or blood by intentionally applying pressure on the neck, throat or chest of another person by any means or to intentionally block the nose or mouth of another person by any means.</p>
--	--

<p>Missouri</p>	<p style="text-align: center;">Mo. REV. STAT. § 565.073. DOMESTIC ASSAULT, SECOND DEGREE – PENALTY ENACTED AND/OR EFFECTED: 2000</p> <p>1. A person commits the offense of domestic assault in the second degree if the act involves a domestic victim, as the term “domestic victim” is defined under section 565.002, and he or she:</p> <ul style="list-style-type: none"> (1) Knowingly causes physical injury to such family or household member by any means, including but not limited to, use of a deadly weapon or dangerous instrument, or by choking or strangulation; or (2) Recklessly causes serious physical injury to such family or household member; or (3) Recklessly causes physical injury to such family or household member by means of any deadly weapon. <p>2. The offense of domestic assault in the second degree is a class D felony.</p>
<p>Montana</p>	<p style="text-align: center;">MT. STAT. §40-5-215 Strangulation of partner or family member ENACTED AND/OR EFFECTED: 2017</p> <p>(1) A person commits the offense of strangulation of a partner or family member if the person purposely or knowingly impedes the normal breathing or circulation of the blood of a partner or family member by:</p> <ul style="list-style-type: none"> (a) Applying pressure on the throat or neck of the partner or family member; or (b) Blocking air flow to the nose or mouth of the partner or family. <p>(2)(a) A person convicted of a first offense of strangulation of a partner or family member shall be fined an amount not to exceed \$50,000 or be imprisoned in the state prison for a term not to exceed 5 years, or both;</p> <p>(b) A person convicted of a second or subsequent offense under this section shall be imprisoned in the state prison for a term of not less than 2 years or more than 20 years and may be fined an</p>

amount not more than \$50,000, except as provided in 46-18-219 and 46-18-222.

(3) A person convicted of strangulation of a partner or family member is required to pay for and complete a counseling assessment as required in 45-5-206(4).

(4) For the purposes of this section, “partner” and “family member” have the meanings provided in 45-5-206.

MT. STAT. §41-3-301. EMERGENCY PROTECTIVE SERVICES

(1) Any child protective social worker of the department, a peace officer, or the county attorney who has reason to believe any child is in immediate or apparent danger of harm may immediately remove the child and place the child in a protective facility. After ensuring that the child is safe, the department may make a request for further assistance from the law enforcement agency or take appropriate legal action. The person or agency placing the child shall notify the parents, parent, guardian, or other person having physical or legal custody of the child of the placement at the time the placement is made or as soon after placement as possible. Notification under this subsection must include the reason for removal, information regarding the show cause hearing, and the purpose of the show cause hearing and must advise the parents, parent, guardian, or other person having physical or legal custody of the child that the parents, parent, guardian, or other person may have a support person present during any in-person meeting with the social worker concerning emergency protective services.

(2) If a social worker of the department, a peace officer, or the county attorney determines in an investigation of abuse or neglect of a child that the child is in danger because of the occurrence of partner or family member assault, as provided for in 45-5-206, or strangulation of a partner or family member, as

	<p>provided for in 45-5-215, against an adult member of the household or that the child needs protection as a result of the occurrence of partner or family member assault or strangulation of a partner or family member against an adult member of the household, the department shall take appropriate steps for the protection of the child, which may include:</p> <p>(a) making reasonable efforts to protect the child and prevent the removal of the child from the parent or guardian who is a victim of alleged partner or family member assault or strangulation of a partner or family member;</p> <p>(b) making reasonable efforts to remove the person who allegedly committed the partner or family member assault or strangulation of a partner or family member from the child's residence if it is determined that the child or another family or household member is in danger of partner or family member assault or strangulation of a partner or family member; and</p> <p>(c) providing services to help protect the child from being placed with or having unsupervised visitation with the person alleged to have committed partner or family member assault or strangulation of a partner or family member until the department determines that the alleged offender has met conditions considered necessary to protect the safety of the child</p> <p>(3) If the department determines that an adult member of the household is the victim of partner or family member assault or strangulation of a partner or family member, the department shall provide the adult victim with a referral to a domestic violence program.</p> <p>(4) A child who has been removed from the child's home or any other place for the child's protection or care may not be placed in a jail.</p> <p>(5) The department may locate and contact extended family members upon placement of a child in out-of-</p>
--	--

	<p>home care. The department may share information with extended family members for placement and case planning purposes.</p> <p>(6) If a child is removed from the child's home by the department, a child protective social worker shall submit an affidavit regarding the circumstances of the emergency removal to the county attorney and provide a copy of the affidavit to the parents or guardian, if possible, within 2 working days of the emergency removal. An abuse and neglect petition must be filed within 5 working days, excluding weekends and holidays, of the emergency removal of a child unless arrangements acceptable to the agency for the care of the child have been made by the parents or voluntary protective services are provided pursuant to 41-3-302.</p> <p>(7) Except as provided in the federal Indian Child Welfare Act, if applicable, a show cause hearing must be held within 20 days of the filing of the petition unless otherwise stipulated by the parties pursuant to 41-3-434.</p> <p>(8) If the department determines that a petition for immediate protection and emergency protective services must be filed to protect the safety of the child, the social worker shall interview the parents of the child to whom the petition pertains, if the parents are reasonably available, before the petition may be filed. The district court may immediately issue an order for immediate protection of the child.</p> <p>(9) The department shall make the necessary arrangements for the child's well-being as are required prior to the court hearing.</p>
--	--

<p>Nebraska</p>	<p align="center">NEB. REV. STAT. ANN. § 28-310.01. STRANGULATION; PENALTY; AFFIRMATIVE DEFENSE ENACTED AND/OR EFFECTED: 2004</p> <p>(1) A person commits the offense of strangulation if the person knowingly or intentionally impedes the normal breathing or circulation of the blood of another person by applying pressure on the throat or neck of the other person.</p> <p>(2) Except as provided in subsection (3) of this section, strangulation is a Class IV felony.</p> <p>(3) Strangulation is a Class III felony if:</p> <ul style="list-style-type: none"> (a) The person used or attempted to use a dangerous instrument while committing the offense; (b) The person caused serious bodily injury to the other person while committing the offense; or (c) The person has been previously convicted of strangulation. <p>(4) It is an affirmative defense that an act constituting strangulation was the result of a legitimate medical procedure.</p>
<p>Nevada</p>	<p align="center">NEV. REV. STAT. ANN. § 200. BATTERY: DEFINITIONS; PENALTIES ENACTED AND/OR EFFECTED: 2009</p> <p>1. As used in this section:</p> <p>(a) “Battery” means any willful and unlawful use of force or violence upon the person of another.</p> <p>(h) “Strangulation” means intentionally impeding the normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person in a manner that creates a risk of death or substantial bodily harm.</p> <p>Nev. Stat. § 200.400(4)(a) Category A felony—Battery with intent to commit sexual assault. Penalties: A person who is convicted of battery with the intent to commit sexual assault shall be punished: (a) If the crime results in substantial bodily harm to the victim or is committed by strangulation, for a category A felony by imprisonment in the state prison: (1) For life without the possibility of parole; or (2) For life with the possibility of parole, with eligibility for parole beginning when a minimum of 10 years has been served, as determined by the verdict of the jury, or the judgment of the court if there is no jury.</p> <p>Nev. Stat. § 193.166(4) Additional penalty: Felony committed in violation of order for protection or order to restrict conduct;</p>

restriction on probation 4. The court shall not grant probation to or suspend the sentence of any person convicted of attempted murder, battery which involves the use of a deadly weapon, battery which results in substantial bodily harm or battery which is committed by strangulation as described in NRS 200.481 or 200.485 if an additional term of imprisonment may be imposed for that primary offense pursuant to this section.

Nev. Stat. § 200.485(2)

Category C felony - Battery which constitutes domestic violence: Penalties; referring child for counseling; restriction against dismissal, probation and suspension; definitions 2. Unless a greater penalty is provided pursuant to NRS 200.481, a person convicted of a battery which constitutes domestic violence pursuant to NRS 33.018, if the battery is committed by strangulation as described in NRS 200.481, is guilty of a category C felony and shall be punished as provided in NRS 193.130 and by a fine of not more than \$15,000.

Nevada Revised Statutes § 178.484 - Right to bail before conviction

(7) A person arrested for a battery that constitutes domestic violence pursuant to NRS 33.018 must not be admitted to bail sooner than 12 hours after arrest. If the person is admitted to bail more than 12 hours after arrest, without appearing personally before a magistrate or without the amount of bail having been otherwise set by a magistrate or a court, the amount of bail must be:

(a) Three thousand dollars, if the person has no previous convictions of battery that constitute domestic violence pursuant to NRS 33.018 and there is no reason to believe that the battery for which the person has been arrested resulted in substantial bodily harm or was committed by strangulation;

(b) Five thousand dollars, if the person has:

(1) No previous convictions of battery that constitute domestic violence pursuant to NRS 33.018, but there is reason to believe that the battery for which the person has been arrested resulted in substantial bodily harm or was committed by strangulation;

or

(2) One previous conviction of battery that constitutes domestic violence pursuant to NRS 33.018, but there is no reason to believe that the battery for which the person has been arrested resulted in substantial bodily harm or was committed by

	<p>strangulation; or</p> <p>(c) Fifteen thousand dollars, if the person has:</p> <p>(1) One previous conviction of battery that constitutes domestic violence pursuant to NRS 33.018 and there is reason to believe that the battery for which the person has been arrested resulted in substantial bodily harm or was committed by strangulation</p>
--	---

<p>New Hampshire</p>	<p>N.H. REV. STAT. ANN. § 631:2. SECOND DEGREE ASSAULT. ENACTED AND/OR EFFECTED: 2010</p> <p>I. A person is guilty of a class B felony if he or she: (f) Purposely or knowingly engages in the strangulation of another.</p> <p>II. In this section: (c) "Strangulation" means the application of pressure to another person's throat or neck, or the blocking of the person's nose or mouth, that causes the person to experience impeded breathing or blood circulation or a change in voice.</p>
<p>New Jersey</p>	<p>N.J. P.L.2018, CHAPTER 53 ENACTED AND/OR EFFECTED: 2017</p> <p>(13) Knowingly or, under circumstances manifesting extreme indifference to the value of human life, recklessly obstructs the breathing or blood circulation of a person who, with respect to the actor, meets the definition of a victim of domestic violence, as defined in subsection d. of section 3 of P.L.1991, c. 261 (C.2C:25-19), by applying pressure on the throat or neck or blocking the nose or mouth of such person, thereby causing or attempting to cause bodily injury.</p> <p>Aggravated assault under paragraphs (1) and (6) of subsection b. of this section is a crime of the second degree; under paragraphs (2), (7), (9) and (10) of subsection b. of this section is a crime of the third degree; under paragraphs (3) and (4) of subsection b. of this section is a crime of the fourth degree; and under paragraph (5) of subsection b. of this section is a crime of the third degree if the victim suffers bodily injury, otherwise it is a crime of the fourth degree. Aggravated assault under paragraph (8) of subsection b. of this section is a crime of the third degree if the victim suffers bodily injury; if the victim suffers significant bodily injury or serious bodily injury it is a crime of the second degree. Aggravated assault under paragraph (11) of subsection b. of this section is a crime of the third degree. Aggravated assault under paragraph (12) or (13) of subsection b. of this section is a crime of the third degree but the presumption of non-imprisonment set forth in subsection e. of</p>

	N.J.S.2C:44-1 for a first offense of a crime of the third degree shall not apply.
--	---

<p>New Mexico</p>	<p style="text-align: center;">N.M.S.A. 1978, § 30-3-16 Aggravated battery against a household member ENACTED AND/OR EFFECTED: 2018</p> <p>A. Aggravated battery against a household member consists of the unlawful touching or application of force to the person of a household member with intent to injure that person or another.</p> <p>B. Whoever commits aggravated battery against a household member is guilty of a misdemeanor if the aggravated battery against a household member is committed by inflicting an injury to that person that is not likely to cause death or great bodily harm, but that does cause painful temporary disfigurement or temporary loss or impairment of the functions of any member or organ of the body.</p> <p>C. Whoever commits aggravated battery against a household member is guilty of a third-degree felony if the aggravated battery against a household member is committed:</p> <ul style="list-style-type: none"> (1) by inflicting great bodily harm; (2) with a deadly weapon; (3) by strangulation or suffocation; or (4) in any manner whereby, great bodily harm or death can be inflicted. <p>D. Upon conviction pursuant to Subsection B of this section, an offender shall be required to participate in and complete a domestic violence offender treatment or intervention program approved by the children, youth and families department pursuant to rules promulgated by the department that define the criteria for such programs.</p> <p>E. Notwithstanding any provision of law to the contrary, if a sentence imposed pursuant to the provisions of Subsection B of this section is suspended or deferred in whole or in part, the period of probation may extend beyond three hundred sixty-four days but may not exceed two years. If an offender violates a condition of probation, the court may impose any sentence that the court could originally have imposed and credit shall not be given for time served by the offender on probation; provided that the total period of incarceration shall not exceed three hundred sixty-four days and the combined period of incarceration and probation shall not exceed two years.</p>
<p>New York</p>	<p style="text-align: center;">ALL ENACTED AND/OR EFFECTED: 2010</p> <p style="text-align: center;">N.Y. PENAL LAW § 121.11 CRIMINAL OBSTRUCTION OF BREATHING OR BLOOD CIRCULATION</p> <p>A person is guilty of criminal obstruction of breathing or blood circulation when, with intent to impede the normal breathing or circulation of the blood of another person, he or she:</p>

	<p>a. applies pressure on the throat or neck of such person; or b. blocks the nose or mouth of such person. Criminal obstruction of breathing or blood circulation is a class A misdemeanor.</p> <p style="text-align: center;">§ 121.12 Strangulation in the second degree</p> <p>A person is guilty of strangulation in the second degree when he or she commits the crime of criminal obstruction of breathing or blood circulation, as defined in section 121.11 of this article, and thereby causes stupor, loss of consciousness for any period of time, or any other physical injury or impairment.</p> <p>Strangulation in the second degree is a class D felony.</p> <p style="text-align: center;">§ 121.13 Strangulation in the first degree</p> <p>A person is guilty of strangulation in the first degree when he or she commits the crime of criminal obstruction of breathing or blood circulation, as defined in section 121.11 of this article, and thereby causes serious physical injury to such other person.</p> <p>Strangulation in the first degree is a class C felony.</p>
--	---

<p>North Carolina</p>	<p>N.C. GEN. STAT. § 14-32.4. ASSAULT INFLECTING SERIOUS BODILY INJURY; STRANGULATION; PENALTIES ENACTED AND/OR EFFECTED: 2004</p> <p>(a) Unless the conduct is covered under some other provision of law providing greater punishment, any person who assaults another person and inflicts serious bodily injury is guilty of a Class F felony. "Serious bodily injury" is defined as bodily injury that creates a substantial risk of death, or that causes serious permanent disfigurement, coma, a permanent or protracted condition that causes extreme pain, or permanent or protracted loss or impairment of the function of any bodily member or organ, or that results in prolonged hospitalization.</p> <p>(b) Unless the conduct is covered under some other provision of law providing greater punishment, any person who assaults another person and inflicts physical injury by strangulation is guilty of a Class H felony.</p>
<p>North Dakota</p>	<p>N.D. § 12.1-17-02. ENACTED AND/OR EFFECTED: 2007</p> <p>1. Except as provided in subsection 2, a person is guilty of a class C felony if that person:</p> <ol style="list-style-type: none"> a. Willfully causes serious bodily injury to another human being; b. Knowingly causes bodily injury or substantial bodily injury to another human being with a dangerous weapon or other weapon, the possession of which under the circumstances indicates an intent or readiness to inflict serious bodily injury; c. Causes bodily injury or substantial bodily injury to another human being while attempting to inflict serious bodily injury on any human being; <p>2. The person is guilty of a class B felony if the person violates subsection 1 and the victim:</p> <ol style="list-style-type: none"> a. Is under twelve years of age; b. Is a peace officer or correctional institution employee acting in an official capacity, which the actor knows to be a fact; or c. Suffers permanent loss or impairment of the function of a bodily member or organ. <p>N.D. Cent. Code Ann. § 12.1-01-04</p> <p>27. "Serious bodily injury" means bodily injury that creates a substantial risk of death or which causes serious permanent disfigurement, unconsciousness, extreme pain, permanent loss or</p>

	<p>impairment of the function of any bodily member or organ, a bone fracture, or impediment of air flow or blood flow to the brain or lungs.</p> <p>29. "Substantial bodily injury" means a substantial temporary disfigurement, loss, or impairment of the function of any bodily member or organ.</p>
--	---

<p>Ohio</p>	<p align="center">ORC § 2919.251- CONSIDERATIONS IN SETTING BAIL IN DOMESTIC VIOLENCE CASES ENACTED AND/OR EFFECTED: 2006 BAIL ONLY</p> <p>(B) To the extent that information about any of the following is available to the court, the court shall consider all of the following, in addition to any other circumstances considered by the court and notwithstanding any provisions to the contrary contained in Criminal Rule 46, before setting bail for a person who appears before the court pursuant to division (A) of this section:</p> <ol style="list-style-type: none"> (1) Whether the person has a history of domestic violence or a history of other violent acts; (2) The mental health of the person; (3) Whether the person has a history of violating orders of any court or governmental entity; (4) Whether the person is potentially a threat to any other person; (5) Whether the person has access to deadly weapons or a history of using deadly weapons; (6) Whether the person has a history of abusing alcohol or any controlled substance; (7) The severity of the alleged violence that is the basis of the offense, including but not limited to, the duration of the alleged violent incident, and whether the alleged violent incident involved serious physical injury, sexual assault, strangulation, abuse during the alleged victim's pregnancy, abuse of pets, or forcible entry to gain access to the alleged victim; (8) Whether a separation of the person from the alleged victim or a termination of the relationship between the person and the alleged victim has recently occurred or is pending; (9) Whether the person has exhibited obsessive or controlling behaviors toward the alleged victim, including but not limited to, stalking, surveillance, or isolation of the alleged victim; (10) Whether the person has expressed suicidal or homicidal ideations; (11) Any information contained in the complaint and any police reports, affidavits, or other documents accompanying the complaint.
<p>Oklahoma</p>	<p align="center">OKLA. STAT. ANN. TIT. 21 § 641. ASSAULT DEFINED ENACTED AND/OR EFFECTED: 2004</p> <p>An assault is any willful and unlawful attempt or offer with force or violence to do a corporal hurt to another.</p>

OKLA. STAT. ANN TIT. 21, § 644. ASSAULT, ASSAULT AND BATTERY, DOMESTIC ABUSE

J. Any person who commits any assault and battery with intent to cause great bodily harm by strangulation or attempted strangulation against a current or former spouse, a present spouse of a former spouse, a former spouse of a present spouse, parents, a foster parent, a child, a person otherwise related by blood or marriage, a person with whom the defendant is or was in a dating relationship as defined by Section 60.1 of Title 22 of the Oklahoma Statutes, an individual with whom the defendant has had a child, a person who formerly lived in the same household as the defendant, or a person living in the same household as the defendant shall, upon conviction, be guilty of domestic abuse by strangulation and shall be punished by imprisonment in the custody of the Department of Corrections for a period of not less than one (1) year nor more than three (3) years, or by a fine of not more than Three Thousand Dollars (\$3,000.00), or by both such fine and imprisonment. Upon a second or subsequent conviction for a violation of this section, the defendant shall be punished by imprisonment in the custody of the Department of Corrections for a period of not less than three (3) years nor more than ten (10) years, or by a fine of not more than Twenty Thousand Dollars (\$20,000.00), or by both such fine and imprisonment. The provisions of Section 51.1 of this title shall apply to any second or subsequent conviction of a violation of this subsection. **As used in this subsection, “strangulation” means** any form of asphyxia; including, but not limited to, asphyxia characterized by closure of the blood vessels or air passages of the neck as a result of external pressure on the neck or the closure of the nostrils or mouth as a result of external pressure on the head.

<p>Oregon</p>	<p style="text-align: center;">OR. REV. STAT. § 163.187. CRIMES AND PUNISHMENTS- STRANGULATION ENACTED AND/OR EFFECTED: 2003</p> <p>(1) A person commits the crime of strangulation if the person knowingly impedes the normal breathing or circulation of the blood of another person by:</p> <ul style="list-style-type: none">(a) Applying pressure on the throat or neck of the other person; or(b) Blocking the nose or mouth of the other person. <p>(2) Subsection (1) of this section does not apply to legitimate medical or dental procedures or good faith practices of a religious belief.</p> <p>(3) Strangulation is a Class A misdemeanor.</p> <p>(4) Notwithstanding subsection (3) of this section, strangulation is a Class C felony if:</p> <ul style="list-style-type: none">(a) The crime is committed in the immediate presence of, or is witnessed by, the person's or the victim's minor child or stepchild or a minor child residing within the household of the person or the victim;(b) The victim is under 10 years of age;(c) During the commission of the crime, the person used, attempted to use or threatened to use a dangerous or deadly weapon, as those terms are defined in ORS 161.015, unlawfully against another;(d) The person has been previously convicted of violating this section or of committing an equivalent crime in another jurisdiction;(e) The person has been previously convicted of violating this section or ORS 163.160, 163.165, 163.175, 163.175, 163.185, or 163.90, or for committing an equivalent crime in another jurisdiction, and the victim in the previous conviction is the same person who is the victim of the current conviction; or
----------------------	--

	<p>(f) The person has at least three previous convictions of any combination of ORS 163.160, 163.165, 163.175, 163.175, 163.185, or 163.90, or of equivalent crimes in other jurisdictions.</p> <p>(5) For purposes of subsection (4)(a) of this section, a strangulation is witnessed if the strangulation is seen or directly perceived in any other manner by the child.</p> <p style="text-align: center;">Senate Bill 1562; Amends ORS § 163.187 ENACTED AND/OR EFFECTED: 2018</p> <p>Carries a maximum prison sentence of 5 years and maximum fine of \$125,000. SB 1562 expands the statutory definition of strangulation to include applying pressure to the chest of the victim. The bill also increases the penalty for strangulation, when the victim is a “family or household member,” or when it is in the context of domestic violence, to a Class C felony.</p>
--	--

<p>Pennsylvania</p>	<p style="text-align: center;">TITLE 18 § 2718. STRANGULATION ENACTED AND/OR EFFECTED: 2016</p> <p>a) Offense defined. --A person commits the offense of strangulation if the person knowingly or intentionally impedes the breathing or circulation of the blood of another person by:</p> <ul style="list-style-type: none">(1) applying pressure to the throat or neck; or(2) blocking the nose and mouth of the person. <p>(b) Physical injury. --Infliction of a physical injury to a victim shall not be an element of the offense. The lack of physical injury to a victim shall not be a defense in a prosecution under this section.</p> <p>(c) Affirmative defense. --It shall be an affirmative defense to a charge under this section that the victim consented to the defendant's actions as provided under section 311 (relating to consent).</p> <p>(d) Grading. --</p> <ul style="list-style-type: none">(1) Except as provided in paragraph (2) or (3), a violation of this section shall constitute a misdemeanor of the second degree.(2) A violation of this section shall constitute a felony of the second degree if committed:<ul style="list-style-type: none">(i) against a family or household member as defined in 23 Pa.C.S. § 6102 (relating to definitions);(ii) by a caretaker against a care-dependent person; or(iii) in conjunction with sexual violence as defined in 42 Pa.C.S. § 62A03 (relating to definitions) or conduct constituting a crime under section 2709.1 (relating to stalking) or Subchapter B of Chapter 30 (relating to prosecution of human trafficking).(3) A violation of this section shall constitute a felony of the first degree if:<ul style="list-style-type: none">(i) at the time of commission of the offense, the defendant is subject to an active protection from abuse order under 23 Pa.C.S. Ch. 61 (relating to protection from abuse) or a sexual violence or intimidation protection order under 42 Pa.C.S. Ch. 62A (relating to protection of victims of sexual violence or intimidation) that covers the victim;(ii) the defendant uses an instrument of crime as defined in section 907 (relating to possessing instruments of crime) in commission of the offense under this section; or(iii) the defendant has previously been convicted of an offense under paragraph (2) or a substantially similar offense in another jurisdiction.
----------------------------	--

<p>Rhode Island</p>	<p style="text-align: center;">GEN. LAWS § 11-5-2.3 DOMESTIC ASSAULT BY STRANGULATION. ENACTED AND/OR EFFECTED: 2012</p> <p>(a) Every person who shall make an assault or battery, or both, by strangulation, on a family or household member as defined in subsection 12-29-2(b), shall be punished by imprisonment for not more than ten (10) years.</p> <p>(b) Where the provisions of “The Domestic Violence Prevention Act”, chapter 29 of title 12, are applicable, the penalties for violation of this section shall also include the penalties as provided in § 12-29-5.</p> <p>(c) “Strangulation” means knowingly and intentionally impeding normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person, with the intent to cause that person harm.</p>
<p>South Dakota</p>	<p style="text-align: center;">SDCL. § 22-18-1.1. AGGRAVATED ASSAULT—FELONY ENACTED AND/OR EFFECTED: 2012</p> <p>Any person who:</p> <p>(8) Attempts to induce a fear of death or imminent serious bodily harm by impeding the normal breathing or circulation of the blood of another person by applying pressure on the throat or neck, or by blocking the nose and mouth;</p> <p>is guilty of aggravated assault. Aggravated assault is a Class 3 felony.</p>
<p>Tennessee</p>	<p style="text-align: center;">TENN. CODE ANN. § 39-13-102. AGGRAVATED ASSAULT ENACTED AND/OR EFFECTED: 2011</p> <p>(a)(1) A person commits aggravated assault who:</p>

	<p>(A) Intentionally or knowingly commits an assault as defined in § 39-13-101, and the assault: (iv) Was intended to cause bodily injury to another by strangulation or bodily injury by strangulation was attempted;</p> <p>(2) For purposes of subdivision (a)(1)(A)(iii) “strangulation” means intentionally impeding normal breathing or circulation of the blood by applying pressure to the throat or neck or by blocking the nose and mouth of another person.</p> <p>(e)(1)(A) Aggravated assault under: (ii) Subdivision (a)(1)(A)(i), (iii), or (iv) is a Class C felony; (iii) Subdivision (a)(1)(A)(ii) is a Class C felony;</p> <p style="text-align: center;">TENN. CODE AMEND. BILL 428 ENACTED AND/OR EFFECTED: 2015</p> <p>a person commits assault, an assault is considered to be aggravated assault, and a Class C felony, if the person intentionally or knowingly commits assault, and such assault was intended to cause bodily injury to another by strangulation or bodily injury by strangulation was attempted. This bill removes the requirement that there be an intent to cause bodily injury in regard to an assault involving strangulation. Under this bill, aggravated assault, where the defendant knowingly or intentionally committed assault and the assault involved strangulation or attempted strangulation, will be a Class C felony. If the defendant recklessly commits an assault and the assault involved strangulation, the offense will be a Class D felony.</p>
--	--

<p>Texas</p>	<p style="text-align: center;">TEX. PENAL CODE ANN. § 22.01. ASSAULTIVE OFFENSES ENACTED AND/OR EFFECTED: 2009</p> <p>(a) A person commits an offense if the person:</p> <ul style="list-style-type: none"> (1) intentionally, knowingly, or recklessly causes bodily injury to another, including the person's spouse; (2) intentionally or knowingly threatens another with imminent bodily injury, including the person's spouse; or (3) intentionally or knowingly causes physical contact with another when the person knows or should reasonably believe that the other will regard the contact as offensive or provocative. <p>(b) An offense under Subsection (a)(1) is a Class A misdemeanor, except that the offense is a felony of the third degree if the offense is committed against:</p> <ul style="list-style-type: none"> (2) a person whose relationship to or association with the defendant is described by Section 71.0021(b), 71.003, or 71.005, Family Code, if: <ul style="list-style-type: none"> (B) the offense is committed by intentionally, knowingly, or recklessly impeding the normal breathing or circulation of the blood of the person by applying pressure to the person's throat or neck or by blocking the person's nose or mouth; <p>(b-1) Notwithstanding Subsection (b)(2), an offense under Subsection (a)(1) is a felony of the second degree if:</p> <ul style="list-style-type: none"> (1) the offense is committed against a person whose relationship to or association with the defendant is described by Section 71.0021(b), 71.003, or 71.005, Family Code; (2) it is shown on the trial of the offense that the defendant has been previously convicted of an offense under this chapter, Chapter 19, or Section 20.03, 20.04, or 21.11 against a person whose relationship to or association with the defendant is described by Section 71.0021(b), 71.003, or 71.005, Family Code; and (3) the offense is committed by intentionally, knowingly, or recklessly impeding the normal breathing or circulation of the blood of the person by applying pressure to the person's throat or neck or by blocking the person's nose or mouth. <p>(f) For the purposes of Subsections (b)(2)(A) and (b-1) (2) :</p>
---------------------	--

(1) a defendant has been previously convicted of an offense listed in those subsections committed against a person whose relationship to or association with the defendant is described by Section 71.0021(b), 71.003, or 71.005, Family Code, if the defendant was adjudged guilty of the offense or entered a plea of guilty or nolo contendere in return for a grant of deferred adjudication, regardless of whether the sentence for the offense was ever imposed or whether the sentence was probated and the defendant was subsequently discharged from community supervision; and
(2) a conviction under the laws of another state for an offense containing elements that are substantially similar to the elements of an offense listed in those subsections is a conviction of the offense listed.

(g) If conduct constituting an offense under this section also constitutes an offense under another section of this code, the actor may be prosecuted under either section or both sections.

ORDINANCE: CITY OF BURLESON, TX “EFFECTIVE RESPONSE TO STRANGULATION”
ENACTED AND/OR EFFECTED: 2018

(a) When the act of strangulation is alleged or suspected within the city, the peace officer will summon emergency medical personnel to the scene to evaluate and render aid to the victim.

(b) The peace officer will document emergency medical personnel’s presence and role in the police report by including their name, identification number, employment agency, and unit number.

(c) Peace officers will thoroughly document the suspect’s behavior, actions, and any comments made during the act of strangulation.

(d) Peace officers will thoroughly document the suspect’s behavior, actions, and any comments made during the act of strangulation.

(e) When the act of strangulation is alleged or suspected within the city, peace officers shall utilize a

	<p>checklist approved by the Chief of Police to help evaluate the situation and provide aid to the victim.</p> <p>(f) When the act of strangulation is alleged or suspected within the city, emergency medical personnel shall conduct a medical evaluation and assessment to help evaluate the situation and provide aid to the victim.</p>
--	--

<p>Utah</p>	<p style="text-align: center;">Utah Code §§ 76-5-103 – Aggravated Assault Penalties ENACTED AND/OR EFFECTED: 2017</p> <ol style="list-style-type: none">1. Aggravated assault is an actor's conduct<ol style="list-style-type: none">a. That is:<ol style="list-style-type: none">i. An attempt, with unlawful force or violence to do bodily injury to another;ii. A threat, accompanied by a show of immediate force or violence, to do bodily injury to another or;iii. An act, committed with unlawful force or violence, that causes bodily injury to another or creates a substantial risk of bodily injury to another; andb. That includes the use of:<ol style="list-style-type: none">i. A dangerous weapons as defined Section 76-1-601;ii. Any act that impedes the breathing or the circulation of blood of another person by the actor's use of unlawful force or violence that is likely to produce a loss of consciousness by:<ol style="list-style-type: none">A. Applying pressure to the neck or throat of a person; orB. Obstruction the nose, mouth, or airway of a person; oriii. Other means or force likely to produce death or serious bodily injury2. Any act under this section is punishable as a third-degree felony, except that an act under this section is punishable as a second-degree felony if:<ol style="list-style-type: none">a. The act results in serious bodily injury; orb. An act under subsection (1)(b)(ii) produces a loss of consciousness <p style="text-align: center;">Utah Code §§ 76-5-103 – Child Abuse—Child Abandonment ENACTED AND/OR EFFECTED: 2017</p> <ol style="list-style-type: none">(i) "Serious physical injury" means any physical injury or set of injuries that:<ol style="list-style-type: none">(A) seriously impairs the child's health;(B) involves physical torture;(C) causes serious emotional harm to the child; or(D) involves a substantial risk of death to the child.(ii) "Serious physical injury" includes:
--------------------	---

	<ul style="list-style-type: none">(B) intracranial bleeding, swelling or contusion of the brain, whether caused by blows, shaking, or causing the child's head to impact with an object or surface;(D) any injury caused by use of a dangerous weapon as defined in Section 76-1-601;(E) any combination of two or more physical injuries inflicted by the same person, either at the same time or on different occasions;(F) any damage to internal organs of the body;(G) any conduct toward a child that results in severe emotional harm, severe developmental delay or intellectual disability, or severe impairment of the child's ability to function;(I) any impediment of the breathing or the circulation of blood by application of pressure to the neck, throat, or chest, or by the obstruction of the nose or mouth, that is likely to produce a loss of consciousness;(K) unconsciousness caused by the unlawful infliction of a brain injury or unlawfully causing any deprivation of oxygen to the brain.
--	--

<p>Vermont</p>	<p style="text-align: center;">V.S.A. § 1024. AGGRAVATED ASSAULT ENACTED AND/OR EFFECTED: 2006</p> <p>(a) A person is guilty of aggravated assault if the person:</p> <ul style="list-style-type: none">(1) attempts to cause serious bodily injury to another, or causes such injury purposely, knowingly, or recklessly under circumstances manifesting extreme indifference to the value of human life; or(2) attempts to cause or purposely or knowingly causes bodily injury to another with a deadly weapon; or(5) is armed with a deadly weapon and threatens to use the deadly weapon on another person. <p>(b) A person found guilty of violating a provision of subdivision (a)(1) or (2) of this section shall be imprisoned for not more than 15 years or fined not more than \$10,000.00, or both.</p> <p>(c) A person found guilty of violating a provision of subdivision (a)(3), (4), or (5) of this section shall be imprisoned for not more than five years or fined not more than \$5,000.00, or both.</p> <p style="text-align: center;">V.S.A. § 1021. DEFINITIONS</p> <p>For the purpose of this chapter:</p> <ul style="list-style-type: none">(1) "Bodily injury" means physical pain, illness or any impairment of physical condition.(2) "Serious bodily injury" means:<ul style="list-style-type: none">(B) strangulation by intentionally impeding normal breathing or circulation of the blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person.
-----------------------	---

<p>Virginia</p>	<p style="text-align: center;">VA. CODE ANN. § 18.2-51.6. STRANGULATION OF ANOTHER; PENALTY ENACTED AND/OR EFFECTED: 2012</p> <p>Any person who, without consent, impedes the blood circulation or respiration of another person by knowingly, intentionally, and unlawfully applying pressure to the neck of such person resulting in the wounding or bodily injury of such person is guilty of strangulation, a Class 6 felony.</p> <p>HB 2120 Strangulation; admission to bail, alleged victim is a family or household member. Admission to bail; strangulation. Adds strangulation where the alleged victim is a family or household member to the list of crimes charged for which there is a rebuttable presumption against admission to bail.</p>
<p>Washington</p>	<p style="text-align: center;">WASH. REV. CODE ANN. § 9A.36.021. ASSAULT IN THE SECOND DEGREE ENACTED AND/OR EFFECTED: 2007</p> <p>(1) A person is guilty of assault in the second degree if he or she, under circumstances not amounting to assault in the first degree: (g) Assaults another by strangulation or suffocation.</p> <p>(2)(a) Except as provided in (b) of this subsection, assault in the second degree is a class B felony. (b) Assault in the second degree with a finding of sexual motivation under RCW 9.94A.835 or 13.40.135 is a class A felony.</p> <p style="text-align: center;">WASH. REV. CODE ANN. § 9A.04.110. DEFINITIONS</p> <p>(26) “Strangulation” means to compress a person's neck, thereby obstructing the person's blood flow or ability to breathe, or doing so with the intent to obstruct the person's blood flow or ability to breathe;</p> <p>(27) “Suffocation” means to block or impair a person's intake of air at the nose and mouth, whether by smothering or other means, with the intent to obstruct the person's ability to breathe;</p>

<p>West Virginia</p>	<p style="text-align: center;">W.V. §61-2-9d. Strangulation; definitions; penalties ENACTED AND/OR EFFECTED: 2016</p> <p>(a) As used in this section: (1) “Bodily injury” means substantial physical pain, illness or any impairment of physical condition; (2) “Strangle” means knowingly and willfully restricting another person’s air intake or blood flow by the application of pressure on the neck or throat; (3) “Suffocate” means knowingly and willfully restricting the normal breathing or circulation of blood by blocking the nose or mouth of another; and (4) “Asphyxiate” means knowingly and willfully restricting the normal breathing or circulation of blood by the application of pressure on the chest or torso.</p> <p>(b) Any person who strangles another without that person’s consent and thereby causes the other person bodily injury or loss of consciousness is guilty of a felony and, upon conviction thereof, shall be fined not more than \$2,500 or imprisoned in a state correctional facility not less than one year or more than five years, or both fined and imprisoned.</p>
<p>Wisconsin</p>	<p style="text-align: center;">Wis. STAT. ANN. §940.235. STRANGULATION AND SUFFOCATION ENACTED AND/OR EFFECTED: 2008</p> <p>(1) Whoever intentionally impedes the normal breathing or circulation of blood by applying pressure on the throat or neck or by blocking the nose or mouth of another person is guilty of a Class H felony.</p> <p>Whoever violates sub. (1) is guilty of a Class G felony if the actor has a previous conviction under this section or a previous conviction for a violent crime, as defined in s. 939.632(1)(e)1.</p>
<p>Wyoming</p>	<p style="text-align: center;">WYO. STAT. ANN. § 6-2-509. STRANGULATION OF A HOUSEHOLD MEMBER; PENALTY ENACTED AND/OR EFFECTED: 2011</p> <p>(a) A person is guilty of strangulation of a household member if he intentionally and knowingly or recklessly causes or attempts to cause bodily injury to a household member by impeding the</p>

	<p>normal breathing or circulation of blood by:</p> <ul style="list-style-type: none">(i) Applying pressure on the throat or neck of the household member; or(ii) Blocking the nose and mouth of the household member. <p>(b) Strangulation of a household member is a felony punishable by imprisonment for not more than five (5) years.</p> <p>(c) For purposes of this section, “household member” means as defined in W.S. 35-21-102(a)(iv)(A) through (D), (G) and (H).</p>
--	--

<p>U.S. Virgin Islands</p>	<p style="text-align: center;">V.I. CODE ANN. TIT. 14 § 296 ASSAULT IN THE SECOND DEGREE ENACTED AND/OR EFFECTED: 2010</p> <p>Whoever willfully-</p> <p>(3) <u>strangle</u> or attempts to strangle any person in an act of domestic violence; or</p> <p>shall be imprisoned not more than 10 years and if the conviction results from an act of domestic violence, the person shall be fined no less than \$1,000 and shall successfully complete certified mandatory Batters Intervention Program.</p>
<p>Guam</p>	<p style="text-align: center;">Guam § 19.80. Strangulation; Defined & Punished ENACTED AND/OR EFFECTED: 2016</p> <p>(a) A person is guilty of strangulation if he knowingly or intentionally, against the will of another, impedes the normal breathing or circulation of the blood of another by applying pressure to the throat or neck or by blocking the nose or mouth of another.</p> <p>b) Strangulation is a felony of the third degree; provided that any person convicted of strangulation shall not be enforceable for work release or educational programs outside the confines of prison."</p>

<p>Federal</p>	<p style="text-align: center;">TITLE 18 USC § 113; ASSAULT WITHIN MARITIME AND TERRITORIAL JURISDICTION ENACTED AND/OR EFFECTED: 2013</p> <p>(a) Whoever, within the special maritime and territorial jurisdiction of the United States, is guilty of an assault shall be punished as follows:</p> <p>(8) Assault of a spouse, intimate partner, or dating partner by strangling, suffocating, or attempting to strangle or suffocate, by a fine under this title, imprisonment for not more than 10 years, or both.</p> <p>(b) Definitions --In this section—</p> <p>(4) the term “strangling” means intentionally, knowingly, or recklessly impeding the normal breathing or circulation of the blood of a person by applying pressure to the throat or neck, regardless of whether that conduct results in any visible injury or whether there is any intent to kill or protractedly injure the victim; and</p> <p>(5) the term “suffocating” means intentionally, knowingly, or recklessly impeding the normal breathing of a person by covering the mouth of the person, the nose of the person, or both, regardless of whether that conduct results in any visible injury or whether there is any intent to kill or protractedly injure the victim.</p>
-----------------------	---

Tribal	<p style="text-align: center;">COLVILLE CONFEDERATED TRIBES</p> <p>Strangulation: Any person who uses their hands or any other object to impede the normal breathing or circulation of blood by applying pressure on the throat or neck, or obstructing the nose or mouth. Strangulation is a Class A offense.</p>
---------------	--

<p>U.S. Military</p>	<p style="text-align: center;">U.C.M.J. H.R. 5515; National Defense Authorization Act ENACTED AND/OR EFFECTED: 2019</p> <p>“(B) commits an offense under this chapter against any property, including an animal; “(3) with intent to threaten or intimidate a spouse, an intimate partner, or an immediate family member of that person, violates a protection order; “(4) with intent to commit a violent offense against a spouse, an intimate partner, or an immediate family member of that person, violates a protection order; or “(5) assaults a spouse, an intimate partner, or an immediate family member of that person by strangling or suffocating; shall be punished as a court-martial may direct.”.</p> <p>(2) CLERICAL AMENDMENT. The table of sections at the beginning of subchapter X of chapter 47 of such title (the Uniform Code of Military Justice) is amended by inserting after the item relating to section 928a (article 128a) the following new item: “928b. 128b. Domestic violence.”</p> <p>(b) EFFECTIVE DATE. The amendments made by this section shall take effect on January 1, 2019, immediately after the coming into effect of the amendments made by the Military Justice Act of 2016 (division E of Public Law 114–328) as provided in section 5542 of that Act (130 Stat. 2967; 10 U.S.C. 801 note).</p>
-----------------------------	--

Bonta, J. (2002). Offender risk assessment: Guidelines for selection and use. *Criminal Justice and Behavior*, 29(4), 355-379. doi: 10.1177/0093854802029004002

Individuals who work with offenders regularly conduct various assessments on their personal characteristics and potential influence on a situation. The assessment results are important to the professionals (e.g., correctional officers and therapists), as well as offenders and the community because they impact treatment and management decisions. The present author summarizes the knowledge regarding offender risk assessments and recommends the following guidelines for the selection and use of risk instruments to predict recidivism (Bonta, 2002).

1. Assessment of offender risk should be based on actuarial measures of risk

According to Bonta, assessment of offender risk should be based on actuarial measures that are structured, quantitative, and empirically linked to a relevant criterion. Two survey studies, Boothby and Clements (2000) and Gallagher, Somwary, and Ben-Porath's (1999), indicate that professionals in the field of corrections use non-actuarial risk assessment tools (e.g., Minnesota Multiphasic Personality Inventory (MMPI); Rorschach; Gender-Gestalt) to evaluate offenders. Some researchers (e.g., Grove & Meehl, 1996; Harris, Rice, & Cormier, 1998) have previously emphasized that using non-actuarial assessments is unethical. Boothby and Clements (2002) indicated that actuarial assessments specifically developed for evaluating offenders (i.e., the Psychopathy Checklist-Revised (PCL-R), Level of Service Inventory-Revised (LSI-R), and the Violence Risk Appraisal Guide (VRAG)), were used infrequently. Interestingly, couple of studies (i.e., Bonta, Law & Hanson, 1998; Hanson & Bussiere, 1998) using mentally disordered offenders and sex offenders samples show that comparing to clinical assessments, effect sizes for the actuarial instruments are higher in predicting violent and sexual recidivism.

2. Risk assessments should demonstrate predictive validity

While many professionals focus on different psychometric characteristics of test instruments, they should focus on the predictive validity because it forecasts the likelihood reoccurrence of future behaviors (Bonta, 2002). Few studies have addressed the predictive validity of measures (e.g., MMPI-2; MCMI) that are often used with offenders by correctional psychologists. Currently, there is little data on the predictive validity of instruments used to assess risk with the offender population. The HCR-20 is a promising risk assessment tool because three studies (Grann, Belfrage, & Tengstrom, 2000; Douglas, Ogloff, Nicholls, & Grant, 1999; and Kroner & Mils 2001) have demonstrated favorable results with its predictive validity. Nevertheless, forensic and correctional professionals should exercise caution when using risk assessment tools that have not been researched extensively. Other tools (e.g., MMPI) that evaluate offenders' emotional and psychological adjustment are not developed to determine recidivism risk. Therefore, it will not suffice to use these tools when assessing such risk.

3. Use assessment instruments that are directly relevant to criminal behavior

There are two classes of behaviors that are significant within the corrections context: rule violation and psychological instability. These behaviors may or may not be interrelated (e.g., paranoia and assault on staff; severe depression is unrelated to engaging in future violence). Thus, psychological maladjustment does not necessarily lead to deviant behaviors (Bonta, 2002). Results from numerous studies (Gendreau, Little, & Goggin, 1996; Simourd, Bonta, Andrews, & Hoge, 1991; Megargee & Bohn, 1979) reveal that the MMPI does not predict rule-violating behaviors very well when compared to other tools (e.g., PCL-R, LSI-R risk-need instrument). Despite these findings, instruments that measure psychological functioning remain popular because it is related to the graduate training most psychologists received in North America, and

only psychologists are authorized to interpret results generated from these measures. For the purpose of risk assessment, selection of appropriate risk assessment tools should be guided by empirical findings (Bonta, 2002).

4. Select instruments derived from relevant theory

If the risk instruments are based on theories of criminal behavior, assessments can be very valuable to the correctional environment. There are three broad criminal behavior theories: sociological-criminological explanations of crime, psychopathological models, and the social learning perspective. Based on the sociological-criminological theories, criminal activities are resulted from a larger social, political, or economic structure of society (Bonta, 2002). Such perspective, however, does not discuss the assessment of offenders. Moreover, research findings supporting sociological-criminological theories of crime are weak (Andres & Bonta, 1998a). Psychopathological theories state that criminal behavior occurs because of biological, emotional, cognitive, or psychological dysfunction. They are the basis for many validated measures but they do not always predict risk (see Bonta et al.'s 1998 meta-analysis). The social learning model suggests that criminal behavior is learned through interactions between cognitive, emotional, personality, and biological factors, as well as environmental reward-cost possibilities (Bonta, 2002). There is ample empirical evidence that supports the social learning theories (e.g., Gendreau et al., 1996; Andrews & Bonta, 1998a).

Researchers have identified antisocial personality, criminal history, antisocial attitudes, and social support for crime – the “Big Four” factors – that predict criminal behaviors (Andrews & Bonta, 1998a). Secondary factors that are relevant within this type of model include prosocial convention indicators (e.g., employment; education), family relationships, and variables that inhibit or facilitate conventional and antisocial actions (Bonta, 2002). Although few offender

assessment tools are based on theories of crime and delinquency, examples of those that do are the I-Level (Jesness, 1988), Conceptual Level (CL) classification systems (Hunt & Hardt, 1965), the Psychopathy Checklist-Revised (PCL-R) (Hare, 1990), and the Level of Service Inventory-Revised (LSI-R) (Andrews & Bonta, 1995).

Van Voorhis (1994) indicates that research data on I-Level and CL's predictive validity is sparse and it focuses on institutional adjustment instead of criminal recidivism. Harpur and Hare (1994) and Hart, Hare, & Forth (1993) have found good predictive validity of offender recidivism with the PCL-R and other tools that combine PCL-R. At the time of Bonta's writing, the most theoretically based offender assessment instrument is the LSI-R. Additionally, its predictive validity is well established (e.g., Andrews & Bonta, 1995, 1998a; Gendreau, Goggin, & Smith, 2002).

5. Sample multiple domains

The standard to evaluate offender risk should use the multi-domain approach, sampling factors related to criminal behavior. Thus, criminal history, antisocial attitudes and values, antisocial personality, social supports for crime, and other relevant domains should be explored. Some tools that address different categories of factors are the HCR-20, PCL-R, Violence Risk Appraisal Guide (VRAG), and the LSI-R. Many of these assess some factors known to predict criminal behavior; however, they are not developed with the intention of sampling different domains (Bonta, 2002).

6. Assess criminogenic need factors

Presently, there are few assessments that combine dynamic and static risk factors (e.g., age, gender). Those that do combine both are risk-need scales such as the LSI-R (Bonta, 2002). Criminogenic needs are dynamic factors that are related to an individual's criminal behaviors

(Andrews, Bonta, & Hoge 1990). In other words, a change in a person's life is associated with his or her criminal behavior. Literatures have shown that offender recidivism rate decreases when the criminogenic needs are reduced (Andrews & Bonta, 1998a; Andrews, Zinger, et al., 1990). While measures have been developed to evaluate criminogenic needs and there is evidence for their predictive validity, research on their dynamic validity is almost nonexistent. Dynamic validity means that the scores obtained by a specific measure for the second time change with the outcome (Bonta, 2002). For instance, Andrews and Wormith (1984) gave probationers the Criminal Sentiments Scale (CSS) to measure their antisocial attitudes and the subjects were asked to take the test again after six months. The subsequent results show a direct relationship between an increase in pretest scores and recidivism.

Dynamic, risk-needs assessments are important for case management within corrections because staff can monitor changes in offenders and their situations, and how such changes affect their risk for engaging in criminal behaviors (Bonta, 2002).

7. Limit general personality and cognitive tests to the assessment of responsivity

The present author states that personality and cognitive tests should not be used to assess risk for recidivism; however, it could be helpful for responsivity considerations. Specifically, the type of treatment used must be congruent with the offenders' cognitive, personality, and sociocultural characteristics (Andrews, Bonta, & Hoge, 1990; Bonta, 1995). Certain assessment tools (e.g., MMPI; I-Level) may not be good at predicting recidivism, but the areas assessed (e.g., antisocial personality) in the instruments could be relevant to the offenders' risk and criminogenic needs, as well as their level of responsivity. Social and cultural factors are noteworthy as well and require consideration when developing treatment programs specifically tailored to the offender (Bonta, 2002).

8. Use different methods to assess risk and needs

Not one single assessment can perfectly predict risk and there are associated errors. The four common methods of evaluation are paper-and-pencil, file review, interview, and behavioral assessment, with disadvantages for each. For instance, a client may not understand the questions asked in a paper-and-pencil format. Another example is that the interview approach may include the interviewer's bias. To increase predictive validity, the evaluator should implement multiple methods of assessment (Bonta, 2002). In a study conducted by Andrews and colleagues (1985), they found that the correlation between evaluation scores and recidivism strengthens when different types of assessment were used.

9. Exercise professional responsibility and 10. Be nice

The last two guidelines that the current author proposes are reminders for professionals to use assessment instruments responsibly. In particular, professionals who use these tests must be well trained in administration and interpretation of test results. They should also keep abreast of the current knowledge on offender assessment. Lastly, the final guideline emphasizes the use of least restrictive alternative when conducting offender risk assessment and developing a management plan.

DANGER ASSESSMENT

Jacquelyn C. Campbell, PhD, RN
Copyright © 1985, 1988, 2001

Several risk factors have been associated with homicides (murders) of both batterers and battered women in research conducted after the murders have taken place. We cannot predict what will happen in your case, but we would like you to be aware of the danger of homicide in situations of severe battering and for you to see how many of the risk factors apply to your situation.

Using the calendar, please mark the approximate dates during the past year when you were beaten by your husband or partner. Write on that date how bad the incident was according to the following scale:

1. Slapping, pushing; no injuries and/or lasting pain
2. Punching, kicking; bruises, cuts, and/or lasting pain
3. "Beating up"; severe contusions, burns, broken bones
4. Threat to use weapon; head injury, internal injury, permanent injury
5. Use of weapon; wounds from weapon

(If **any** of the descriptions for the higher number apply, use the higher number.)

Mark **Yes** or **No** for each of the following. ("He" refers to your husband, partner, ex-husband, ex-husband, or whoever is current physically hurting you.)

- 1. Has the physical violence increased in severity or frequency over the past year?
 - 2. Has he ever used a weapon against you or threatened you with a weapon?
 - 3. Does he ever try to choke you?
 - 4. Does he own a gun?
 - 5. Has he ever forced you to have sex when you did not wish to do so?
 - 6. Does he use drugs? By drugs, I mean "uppers" or amphetamines, speed, angel dust, cocaine, "crack", street drugs or mixtures.
 - 7. Does he threaten to kill you and/or do you believe he is capable of killing you?
 - 8. Is he drunk every day or almost every day? (In terms of quantity of alcohol.)
 - 9. Does he control most or all of your daily activities? For instance: does he tell you who you can be friends with, when you can see your family, how much money you can use, or when you can take the car? (If he tries, but you do not let him, check here:)
 - 10. Have you ever been beaten by him while you were pregnant? (If you have never been pregnant by him, check here:)
 - 11. Is he violently and constantly jealous of you? (For instance, does he say "If I can't have you, no one can.")
 - 12. Have you ever threatened or tried to commit suicide?
 - 13. Has he ever threatened or tried to commit suicide?
 - 14. Does he threaten to harm your children?
 - 15. Do you have a child that is not his?
 - 16. Is he unemployed?
 - 17. Have you left him during the past year? (If you *never* lived with him, check here:)
 - 18. Do you currently have another (different) intimate partner?
 - 19. Does he follow or spy on you, leave threatening notes, destroy your property, or call you when you don't want him to?
- Total "Yes" Answers

Thank you. Please talk to your nurse, advocate or counselor about what the Danger Assessment means in terms of your situation.

Reference List

- Block, C.R., Engel, B. Naureckas, S.M., & Riordan, K.A. (1999). The Chicago women's health risk study: Lessons in collaboration. Violence Against Women, 5, 1158-1177.
- Campbell, J. (1986). Nursing assessment for risk of homicide with battered women. Advances in Nursing Science, 8, 36-51.
- Campbell, J. (1995). Assessing dangerousness. Newbury Park: Sage.
- Campbell, J., Soeken, K., McFarlane, J., & Parker, B. (1998). Risk factors for femicide among pregnant and nonpregnant battered women. In J.C. Campbell (Ed.), Empowering survivors of abuse: Health care for battered women and their children (pp. 90-97). Thousand Oaks, CA: Sage.
- Diaz-Olavarrieta, C., Campbell, J., Garcia de le Cadena, C., Paz, F., & Villa, A. (1999). Domestic violence against patients with chronic neurologic disorders. Archives of Neurology, 56, 681-685.
- McFarlane, J., Parker, B., Soeken, K., & Bullock, L. (1992). Assessing for abuse during pregnancy: Severity and frequency of injuries and associated entry into prenatal care. JAMA, 267, 3176-3178.
- McFarlane, J., Parker, B., & Soeken, K. (1996). Abuse during pregnancy: Associations with maternal health and infant birth weight. Nursing Research, 45, 37-42.
- McFarlane, J., Soeken, K., Reel, S., Parker, B., & Silva, C. (1997). Resource use by abused women following an intervention program: Associated severity of abuse and reports of abuse ending. Public Health Nursing, 14, 244-250.
- Parker, B., McFarlane, J., & Soeken, K. (1994). Abuse during pregnancy: Effects on maternal complications and birth weight in adult and teenage women. Obstetrics & Gynecology, 84, 323-328.
- Roehl, J. & Guertin, K. (1998). Current use of dangerousness assessments in sentencing domestic violence offenders. Pacific Grove, CA: State Justice Institute.
- Silva, C., McFarlane, J., Soeken, K., Parker, B., & Reel, S. (1997). Symptoms of post-traumatic stress disorder in abused women in a primary care setting. Journal of Women's Health, 6, 543-552.
- Stuart, E.P. & Campbell, J.C. (1989). Assessment of patterns of dangerousness with battered women. Issues Mental Health Nursing, 10, 245-260.
- Websdale, N. (1999). Understanding domestic homicide. Boston: Northeastern.
- Weisz, A., Tolman, R., & Saunders, D.G. Assessing the risk of severe domestic violence: The importance of survivor's predictions. Violence & Victims (in press)
- Woods, S. (1998). Post-traumatic stress disorder in battered women. Unpublished doctoral dissertation, Washington State University.

Rebecca and Bill Exercise – Information and Instructions

<p>Roles:</p>	<ul style="list-style-type: none"> • Probation • Court Staff • Judge • Advocates • Lawyers • GALs • Batterer’s Intervention Program • Law Enforcement
<p>Instructions:</p>	<ul style="list-style-type: none"> • Facts have all been obtained from the record in this case. • Various parties/professionals had different pieces of information. • Throughout the exercise, consider: <ul style="list-style-type: none"> ✓ Who knew what? ✓ When did they know it? ✓ What should have been done? ✓ What is the level of risk to the victim? ✓ What is the level of risk to the court?
<p>Based on a real case: Rebecca and Bill Smith</p>	<p>February 1996: Rebecca and Bill met.</p>

	<p>October 1996: Rebecca and Bill married.</p> <p>April 1997: Son Jared is born.</p>
Assault: April 23, 2002	<p>Law Enforcement Records: Neighbors call police after hearing Rebecca screaming, “You are killing me!” Law Enforcement arrests and charges Bill with domestic assault. At the time, Bill asks officers, “Can you charge her with breaking and entering into my office?”</p>
Same Day: April 23, 2002	<p>Law Enforcement: “At 06:25 hours, advised by Sgt. Craig that Rebecca Smith called and advised that she found tapes in Bill Smith’s office and that he had been tape recording all of her phone conversations.” Bill is brought before the court for pre-trial release.</p>
Level of Risk: LOW/MEDIUM/HIGH	What would you do?
Over the Next 4 days: April 23-27, 2002	<p>Pre-Trial Services strongly opposed bail, based on the information regarding tape recordings of his spouse’s phone calls.</p> <p>The Court released Bill on bail and placed him on pre-trial supervision. Conditions included counseling (if recommended), anger management and a restraining order for Rebecca.</p> <p>Rebecca called police because she was concerned for her safety, “I have a restraining order, but my husband’s brother and other family members keep driving by my house.”</p>

	BIP: Bill attended one BIP session but was removed for being disruptive. Bill denied any wrongdoing regarding Rebecca.
Level of Risk: LOW/MEDIUM/HIGH	What would you do?
Same Day, April 27, 2002	Law Enforcement dispatched to Bill’s current address, no arrest made. Report taken. BIP to Bill, “You can return to BIP anytime.”
10 Days Later: May 13, 2002	Bill Smith, through counsel, filed a Complaint for custody of Jared. Rebecca, through counsel, filed an Answer and asked for full custody. Rebecca stated in the documents that she was, “concerned about her son’s safety and when he is unsupervised with Bill.” She also stated that Bill has multiple guns and she feared his upcoming court date for the criminal charges because it might make him, “more desperate in his actions.”
Over the Next Week: May 13-21, 2002	Based on Rebecca’s allegations, the Court notified CPS. CPS opened an investigation. CPS’ investigation report included statements by Jared, as follows: <ul style="list-style-type: none"> • “My dad is always talking about what happened the night the police came.” • “My dad told me to say that mommy doesn’t take care of me.” • “My dad lies all the time and my uncle pinches me and I don’t like it.”

	<p>CPS investigation report includes statements by Bill that, “I never hit Rebecca.” He denied any fault.</p> <p>CPS investigation report included statements by Rebecca that, “Without going into details, Bill made sure I got pregnant.”</p> <p>CPS investigation report quoted Rebecca, stating: “I asked Bill why he was so cruel to me during the ultrasounds and Bill held up the phone that had is mother on the other end and made fun of me crying to his mother. I ran up to the bathroom and slammed the door. Mr. Smith punched a hole in the kitchen door. He then chased after me, tore down the bathroom door, and yelled at me to never slam a door on him again. He threatened to shoot me. I am in extreme fear. For one month, I have been sleeping with a knife under my bed; I am afraid for my and my son’s safety.”</p>
<p>Level of Risk: LOW/MEDIUM/HIGH</p>	<p>What would you do?</p>
<p>Next Day: May 22, 2002</p>	<p>CPS closed the file, noting no child protection concerns, but sent a letter to both parents stating that, “Jared is fully aware of the assault and both parents have inappropriately exposed Jared to adult issues.” CPS warned of possible future intervention if CPS receives any report of emotional harm to Jared.</p> <p>Family Court issued an interim custody and access order: “Plaintiff (Bill) to have liberal and generous periods of access.”</p>

<p>8 Months Later: January 20, 2003 (Ninth months after assault.)</p>	<p>Bill pleaded guilty to the spousal assault of 4/23/2002. Prosecutor withdrew charge for intercepting private communications from that arrest. Criminal Court suspended sentence, including two years' probation; 75 hours of community service; paying \$300 to a women's shelter; anger management; and no contact with Rebecca.</p>
<p>Starting 2 days later: January 23 – March 12, 2003</p>	<p>Probation had first meeting with Bill. BIP invited Bill to initial registration. BIP invited Bill a second time.</p>
<p>Approximately 10 weeks after guilty plea: April 2, 2003</p>	<p>Bill signed contract with BIP and completed a Power and Control Inventory. BIP report quoted Bill:</p> <ul style="list-style-type: none"> • “Knocking Rebecca down was an accident.” • “I never assaulted her.” <p>BIP report stated that Bill only “rarely” called Rebecca names; put her down, criticized her appearance, intelligence, or abilities; criticized her family; and gave her the silent treatment.</p>
<p>Next Day: April 3, 2003</p>	<p>Probation stated that Bill notified the officer that he registered by BIP, but he expressed concerns that it might interfere with his work schedule. Probation officer told him to work around it.</p>
<p>2 Weeks Later: May 8, 2003</p>	<p>Bill told probation officer that, “BIP interferes with my parenting time.” He also said that Rebecca “sleeps in” often and leaves Jared unsupervised.</p>

	<p>Probation officers received report from Rebecca about May 7, 2003, incident where Bill drove by the house and screamed Jared’s name. She stated that she, “feels intimidated and threatened,” but did not want to press charges.</p>
<p>Level of Risk: LOW/MEDIUM/HIGH</p>	<p>What would you do?</p>
<p>Same Day, May 8, 2003</p>	<p>Probation officer told Bill, “You are trying to control Rebecca by portraying her as a bad mother. You must comply with BIP. Try again.”</p> <p>Probation did not report the drive-by incident and no charges for either the drive-by or the failure to attend BIP.</p>
<p>Later That Month: May 26 – July 16, 2003 (15 months after assault, 6 months after guilty plea)</p>	<p>BIP report quoted Bill as saying,</p> <ul style="list-style-type: none"> • “My only goal is to satisfy probation; I have done nothing wrong.” • To other group members: “I can teach you how to hide money so your ex won’t get it.” • “The system is unfair to men.” • “Rebecca is crazy.” <p>BIP report stated that,</p>

	<ul style="list-style-type: none"> • Bill gave a false name and wrong contact information for a new girlfriend. • Bill admitted to "keeping track" of Rebecca using social media. • Bill refused to give the girlfriend's name repeatedly, telling BIP that it is a matter for probation. <p>BIP removed Bill from the program, but said he could return in the future.</p> <p>BIP told Probation that Bill claimed innocence, alleged the system is against him, is disruptive in group and lies.</p>
2 Weeks Later: August 3 - 5, 2003	<p>Bill told Probation officer that he moved in with the new girlfriend, Lynn, and her 8 year-old daughter, Laura.</p> <p>Probation officer met with BIP to discuss Bill's failure to comply.</p>
About 1 Week Later: August 14, 2003	<p>Probation officer and BIP had further discussions regarding charges for Bill's failure to comply with BIP. BIP expressed concerns about the safety of Bill's current partner, Lynn.</p>
1 Week Later: August 21, 2003	<p>Court record reflects that Rebecca moved for a modification of visitation arrangements and asked the Court to appoint a GAL for Jared.</p>
About 2 Weeks Later: September 4, 2003	<p>Probation officer considered whether to report Bill's failure to attend BIP and the drive-by incident to the Court.</p>

<p>About 1 Week Later: September 12, 2003 (17 months after the assault; 9 months after guilty plea, 2 months after expelled from BIP)</p>	<p>Probation reported violation to Law Enforcement. Law Enforcement arrested Bill for violations of probation and Court anti-harassment Order.</p> <p>Probation notified Rebecca that Bill was in custody.</p>
<p>Level of Risk: LOW/MEDIUM/HIGH</p>	<p>What would you do?</p>
<p>Same Day, September 12, 2003</p>	<p>Criminal Court released Bill on bail.</p>
<p>4 Days Later: September 16, 2003</p>	<p>Law Enforcement receives a call from Rebecca, who states, “I decided to call the police because I know what kind of person Bill is, I am worried about him snapping.” She also reports that she found “hundreds upon hundreds,” of .22 caliber bullets hidden in the laundry room and a gun clip five feet from the furnace. She said the bullets had not been there as recently as the prior month. She told Law Enforcement about how, shortly before she left him, he forced her out of a car and fired a gun at her feet.</p>
<p>Level of Risk: LOW/MEDIUM/HIGH</p>	<p>What would you do?</p>
<p>Same Day, September 16, 2003</p>	<p>Law Enforcement told Rebecca to bring the ammunition to the police station. Law Enforcement notified CPS of Bill’s failure to attend BIP and the drive-by incident of 5/7/2003. CPS begins an investigation based on the new charges.</p>

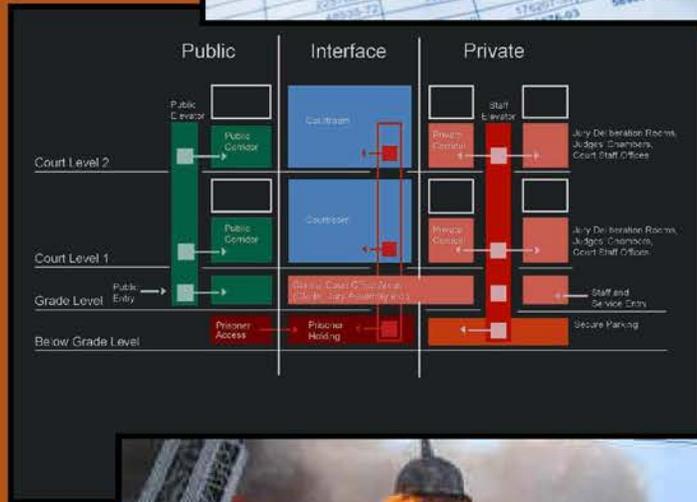
<p>Over the Course of the Next Month: September – October 2003</p>	<p>CPS received information that Bill was kicked out of BIP. Jared complained about visits with Bill to CPS. Bill told Probation officer he was considering giving up access to Jared.</p>
<p>Level of Risk: LOW/MEDIUM/HIGH</p>	<p>What would you do?</p>
<p>Same Period: October 2003</p>	<p>CPS closed the file finding no child protection issue. CPS warned Bill and Rebecca again of the dangers of exposing Jared to adult issues between his parents.</p> <p>Probation officers advised Bill to consider supervised visits with Jared rather than dropping access entirely and recommended that Bill start BIP again.</p>
<p>About 1 Month Later: November 4, 2003</p>	<p>Bill stated to Probation officer that he felt vindicated by CPS.</p>
<p>1 week Later: November 10, 2003</p>	<p>The Court appointed a GAL for Jared.</p>
<p>1 Month Later: December 2003 – January 2004</p>	<p>Probation officer advised Bill to return to BIP.</p> <p>Bill agreed to complete BIP but not with the same provider.</p> <p>Probation also spoke to Bill’s new girlfriend who reported, “no evidence of abusive behavior” from Bill.</p>

	Upon notification from Bill that he was doing an anger management correspondence course, Probation officer recorded that he was “not crazy about it,” but it seemed no worse or better than the last BIP.
1 Month Later: February 2004	Probation officer met with Bill and Bill reported that he, “listens to anger management tapes in the car.”
Level of Risk: LOW/MEDIUM/HIGH	What would you do?
1 Month Later: March 19, 2004 (23 months after the assault; 14 months after guilty plea)	GAL recommended to the Court: <ul style="list-style-type: none"> • Custody to Rebecca • Unsupervised access for Bill • Bill should receive continued treatment on power and control issues and on the effect of DV on children.
4 Months Later: July – September 2004	Probation officer received Bill’s completion letter from the on-line anger management course. Bill told Probation that Rebecca had been calling him but he refused to talk to her, in compliance with the Court order. A new Probation officer took over.
1 Month Later: October 2004	Bill’s girlfriend, Lynn, changed the locks when Bill left for work and Bill then moved in with his mother.

	<p>The Court (family) agreed with the recommendation of the GAL and issued an order of unsupervised access to Jared for Bill.</p>
<p>2 Months Later: December 13, 2004 (2.75 years after the assault; 2 years after guilty plea)</p>	<p>The Court scheduled a hearing based on Rebecca’s petition for a 1-year protection order against Bill (civil). Probation from the April 2002 arrest expired and “all conditions met.”</p> <p>Prior to the hearing, Bill showed up at Lynn’s home. Lynn allowed Bill in the home. Law Enforcement received a call from Lynn and Laura. They fled their home after Bill attacked them.</p> <p>Upon law enforcement arrival at Lynn’s home, Bill was no longer there. He arrived at court for the hearing carrying a gun. He saw Rebecca walking across the street on her way to the hearing, grabbed her, and dragged her into his car. Bill held Rebecca hostage in his car parked in front of the court, threatening to kill her unless he was given custody of Jared. Law Enforcement arrived and shot Bill.</p>

CCJ/COSCA Court Security Handbook

Ten Essential Elements for Court Security and Emergency Preparedness



Prepared Under the Auspices of the
CCJ/COSCA Joint Committee on Court Security and
Emergency Preparedness

CCJ/COSCA

Court Security Handbook

*Ten Essential Elements for Court Security and
Emergency Preparedness*

PUBLISHED JUNE 2010
REVISED SEPTEMBER 2012

**Prepared Under the Auspices of the
CCJ/COSCA Joint Committee on Court Security and
Emergency Preparedness**



Table of Contents

	<u>Page</u>
Dedication	i
Acknowledgements	ii
Essential Ten Elements for Effective Courtroom Safety and Security Planning.....	iv
Introduction.....	v
Strategies for Success	ix
Best Practices Institute: Emergency Management for Courts	x
Chapter One: Standard Operating Procedures	1-1
Chapter Two: The Self-Audit	2-1
Chapter Three: Emergency Preparedness and Response: Continuity of Operations (COOP)	3-1
Chapter Four: Disaster Recovery—Essential Elements of a Plan	4-1
Chapter Five: Threat Assessment	5-1
Chapter Six: Incident Reporting	6-1
Chapter Seven: Funding for Court Security.....	7-1
Chapter Eight: Security Equipment and Costs.....	8-1
Chapter Nine: Resources/Partnerships.....	9-1
Chapter Ten: New Courthouse Design	10-1

Appendices

Appendix A: Representative Sample of Guidelines from State Court Security Manuals	A-1
Appendix B: Steps to Best Practices for Court Building Security	B-1
Appendix C: Home Security Audit and Recommendations	C-1
Appendix D: Model Disaster Recovery Plan Forms.....	D-1
Appendix E: Unified Judicial System of Pennsylvania— Security Incident Fact Sheet	E-1
Appendix F: Sample Memorandum of Understanding.....	F-1

Dedication



Thomas J. Moyer
Chief Justice, Supreme Court of Ohio
April 18, 1939 – April 2, 2010

In 2003 the Conference of Chief Justices and Conference of State Court Administrators established a Committee on Security and Emergency Preparedness. In recognition of the gravity and importance of court security, the Chief Justices designated Tom Moyer to be the committee's first co-chair. From 2003 to his untimely passing in 2010, Chief Justice Moyer served as the committee's co-chair and advanced the interests of judicial security with wisdom, patience and gentility. This practical guide is both a tribute to Chief Justice Moyer and a testament to his remarkable work in the complex field of court security. We are truly the beneficiaries of his pioneering efforts. We dedicate this court security handbook to Chief Justice Thomas Moyer. His many good works will always be remembered.

Acknowledgements

Members of the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA) Committee on Court Security and Emergency Preparedness gratefully acknowledge the assistance of the many individuals who contributed to the publication of this handbook: *CCJ/COSCA Court Security Handbook - Ten Essential Elements for Court Security and Emergency Preparedness*. It is the result of efforts, cooperation, and hard work of many that information contained in these chapters was produced.

Over the years, numerous chief justices and state court administrators who have served on the Committee have contributed their time and energy not only to developing the ten elements, but to putting them into a useable format that judges and court managers can use as guidelines to improve the safety and security of those individuals they serve in our national system of justice.

Members of the Committee from fiscal year from 2009-10 through 2011-12 are:

CCJ Members	COSCA Members
Thomas J. Moyer (dec.) OH, <i>Co-Chair</i>	Zygmunt A. Pines, PA, <i>Co-Chair</i>
Paul L. Reiber, VT, <i>Co-Chair</i>	Karl R. Hade, VA, <i>Co-Vice Chair</i>
Michael L. Douglas, NV, <i>Co-Vice Chair</i>	Arthur W. Pepin, NM, <i>Co-Vice Chair</i>
Sharon Keller, TX, <i>Co-Vice Chair</i>	Joseph Baxter, RI
Sue Bell Cobb, AL	Steven D. Canterbury, WV
James E. Edmondson, OK	Nancy Dixon, KS
Thomas R. Fitzgerald, IL	James T. Glessner, ME
Thomas L. Kilbride, IL	Elisabeth H. Goodner, FL
Marilyn S. Kite, WY	Donald D. Goodnow, NH
Maureen O'Connor, OH	Glenda L. Lake, VI
Paul A. Suttell, RI	Rodney A. Maile, HI
Steven Taylor, OK	Ron Overholt, CA
Barton R. Voigt, WY	Perry C. Taitano, GU
	A. John Voelker, WI
	Anne B. Wicks, DC

We would also like to offer special thanks to our many colleagues, consultants, and court experts for their comments and contributions to the ten chapters contained in this handbook. Those who contributed greatly to the development and publication of this report are reviewers of the handbook — Steve Canterbury, Lisa Goodner, and Pat Griffin

as well as NCSC liaison to the Committee, Timm Fautsko, and former liaisons Carolyn Ortwein and José Dimas. Other contributors are Judy Amidon, Steve Berson, Ephanie Blair, Pam Casey, Tom Clarke, Paul Embley, Kay Farley, Dan Hall, Laura Klaversma, Frank Lalley, Arnold Lum, Jim O’Neil, Kevin Sheehan, Jewel Williams. Special appreciation is extended to Darren Breslin, Alicia Davis, Kären Hallstrom, and Mary Beth Kirven for their development of the section in Chapter Three entitled Emergency Preparedness and Response: Continuity of Operations (COOP).

With respect to the chapters, we have again received contributions from many internal and external contributors for whose efforts we are sincerely grateful. Our gratitude also extends to the many members of the court community who shared information and made suggestions about the application of the ten elements. These contributions are reflected in the content of the chapters and demonstrate the value of networking and collaboration between states’ administrative offices of courts and the practitioners in the field. We would also like to recognize the many sponsors of the Web sites and companies that are listed in the Resources and References section at the end of each chapter.

Essential Ten Elements for Effective Courtroom Safety and Security Planning

As determined by the Joint Committee on Security and Emergency Preparedness of the Conference of Chief Justices and Conference of State Court Administrators in October 2003

1. Operational Security: Standard Operating Procedures

This is one of the most critical deficiencies in the state court system today. Standard Operating Procedures are not being followed and for full safety, there needs to be 100 percent compliance.

2. Facility Security Planning: The Self-Audit Survey of Court Facilities

This point emphasizes the need to know the strengths and weaknesses of the physical structure of the courtroom to best protect the people inside.

3. Emergency Preparedness and Response: Continuity of Operations

At any moment, courts can be affected by natural or unnatural disasters; however, they must continue to operate and serve the public in such an event. There needs to be a greater awareness and identification of command structure, protocols, and communication routes for such emergencies and responses.

4. Disaster Recovery: Essential Elements of a Plan

The point emphasizes the need to ensure that adequate procedures are in place to recover lost or vulnerable information in the event of an emergency.

5. Threat Assessment

The federal government currently has an effective threat assessment protocol in practice. However, for security and safety purposes, state courts need to begin identifying serious threats so they may prepare for the proper protective action.

6. Incident Reporting

States must develop an appropriate incident report form that allows for capturing data on items such as intelligence and funding needs.

7. Funding

This is another critical deficiency facing the court system today and for years past. Equipment can be bought at moderate costs but without the trained personnel, the equipment is of little to no use. In addition, many state court administrators are troubled by the lack of federal funds. While much money is appropriated for homeland security, very little is dedicated to state courts.

8. Security Equipment and Costs

State courts must have updated and readily available information on what technology is available to them and how much it costs.

9. Resources and Partnerships

Strong and effective partnerships among state courts, law enforcement, and county commissioners must be developed to ensure successful security operations.

10. New Courthouse Design

As new courthouses are being constructed, this point emphasizes the opportunity to ensure that up-to-date physical safety measures are included in the design stage.

More on the National Summit on Court Safety and Security (www.ncsconline.org)

The NCSC has secured support and participation of members of Congress, Department of Justice officials, and state and county court officials, as well as members from public safety and state and local governments, in the National Summit. NCSC president Mary McQueen, who has been a strong and vocal leader of the state court community, has promised her members and the communities they serve that the outcome of the Summit will not only provide best practices for improving safety and security, but also use the power of its participants to call for necessary funding to implement such plans. ■

Introduction

The terror attacks on September 11, 2001, produced increased concerns for safety and security for virtually all institutions in this country. State courts were no exception. In 2003, a Court Security and Emergency Preparedness Committee (Committee) was convened by the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA) and included representatives from both. The mission statement of the Committee reads as follows:

Most court managers believe that their facilities will not be targeted for a terrorist attack, or that disaster, natural or man-made, only happens to other people. Yet, as we are all too aware, catastrophic events can happen to anyone, at any time. Hurricanes, floods, fire, and earthquakes, as well as terrorism and civil disorder all threaten the ability of the courts to remain open. The events of September 11, 2001, further illustrated the vulnerability of public institutions and the urgent need for effective emergency response and security. Under Standard 1.2 of the Court Performance Standards – Access to Justice – a court is required to make its facilities safe, accessible, and convenient to use. The joint committee will identify and address key emergency planning, response, and security issues that affect state court systems and which have an impact on the courts' ability to maintain continuity of operations and the rule of law.

In October 2003, the Committee conducted a survey of the states to determine security needs of state courts and to identify effective practices in the area of court security. An analysis of the survey results produced a framework for addressing court safety and security called *Ten Essential Elements for Court Safety and Security*. Those elements were identified and generally defined as

Element 1 - Operational Security: Standard Operating Procedures

This is one of the most critical deficiencies in the state court system today. Standard Operating Procedures are not being following and, for full safety, there needs to be one hundred percent compliance.

Element 2 - Facility Security Planning: The Self-Audit Survey of Court Facilities

This point emphasizes the need to know the strengths and weaknesses of the physical structure of the courtroom so that the people within are best protected.

Element 3 - Emergency Preparedness and Response: Continuity of Operations

At any moment, courts can be affected by natural or manmade disasters; however, they must continue to operate and serve the public in such events. There needs to be a greater awareness and identification of command structure, protocols, and communication routes for such emergencies and responses.

Element 4 - Disaster Recovery: Essential Elements of a Plan

Adequate procedures must be in place to recover lost or vulnerable electronic and other hard copy information in the event of an emergency.

Element 5 - Threat Assessment

The federal government currently has an effective threat assessment protocol in practice. However, for security and safety purposes, state courts need to begin identifying serious threats so they may prepare for the proper protective actions.

Element 6 - Incident Reporting

States must develop an appropriate incident report form that allows for capturing data on items such as intelligence and funding needs.

Element 7 - Funding

This is another critical deficiency facing the court system today and for years past. Equipment can be bought at moderate costs but, without the trained personnel, the equipment is of little to no use. In addition, many state court administrators are troubled by the lack of federal funds. While much money is appropriated to homeland security, very little is dedicated to state courts.

Element 8 - Security Equipment and Costs

State courts must have updated and readily available information on what technology is available to them and how much it costs.

Element 9 - Resources and Partnerships

Strong and effective partnerships among state courts, law enforcement, and county commissioners must be developed to ensure successful security operations.

Element 10 - New Courthouse Design

As new courthouses are being constructed, this point emphasizes the opportunity to ensure that up-to-date physical safety measures are included in the design stage.

The subject matters reflected in these ten elements cover the many issues and concerns that court leadership – judges and court administrators – must consider in discharging their responsibility to provide a safe and secure environment. These topics include the following: making sure policies and procedures are in place to assure safety and security (Element 1); assessing the current level of protection that exists within the courthouse (Element 2); planning to stay open in the face of disaster and recovering data and other resources lost in a disaster (Elements 3 and 4); identifying potential threats and documenting existing threats in order to increase levels of protection (Elements 5 and 6); developing effective funding and partnership strategies to assure the resources necessary to provide a reasonable level of protection (Elements 7, 8, and 9); and building a sufficient level of security into planning for new facilities (Element 10).

Pursuant to the Committee’s mission statement, the subject matters covered by the elements are consistent with those Trial Court Performance Standards (TCPS) relating to security developed by the National Center for State Courts (NCSC) – Access to Justice. Performance Standard 1.2 deals with Safety, Accessibility, and Convenience. The following four measures relate to safety. Measure 1.2.1 examines the physical security of the courthouse with a formal security audit. Measure 1.2.2 requires that trained law enforcement officers conduct a test of courthouse security by observing and trying to breach the court’s security. Measure 1.2.3 uses a survey to assess the general sense of safety perceived by regular users of the court. Measure 1.2.4 examines the training courthouse employees receive with respect to responding to emergency situations.

Since the formulation of the *Ten Essential Elements*, much has happened to fuel interest in and concern for courthouse safety and security. On March 11, 2005, an in-custody defendant in the Fulton County Courthouse in Atlanta, Georgia, overpowered a security officer and fatally shot a judge, a court reporter, a court security officer and, the next day, a customs officer. Many other security incidents since 2005 have served to elevate concerns. Disasters such as Hurricane Katrina, along with fears over such potential disasters as pandemic flu outbreaks (such as H1N1 - Swine Flu), have served to heighten appreciation for the need for continuity of operations planning (COOP) and

disaster recovery. Even lesser and more frequent emergencies such as the facilities-closing blizzards of 2010 are illustrative of the need for a clearly developed COOP.

As a result, a vast amount of information is available on the general subject area of emergency preparedness as well as in much greater detail regarding each of these ten elements. Much of this information can be found online and in hard copy documents published by state judicial departments, federal and state agencies, and various organizations.

Although this handbook is not intended to provide detailed answers to every court security and emergency preparedness question, it does provide the user a convenient yet significant gateway to this information. Contained herein is a chapter on each of the ten elements. Each chapter will offer the reader the following:

- A general discussion of the element: what it encompasses and why it is so important.
- A practical guide on what needs to be done to put the element in place: what are the specific steps to take to assure a reasonable level of protection?
- A list of additional references/resources: where to look for more expansive and detailed information on each element in both hard copy and electronic format on the Internet.

EMERGENCY MANAGEMENT for COURTS Strategies for Success

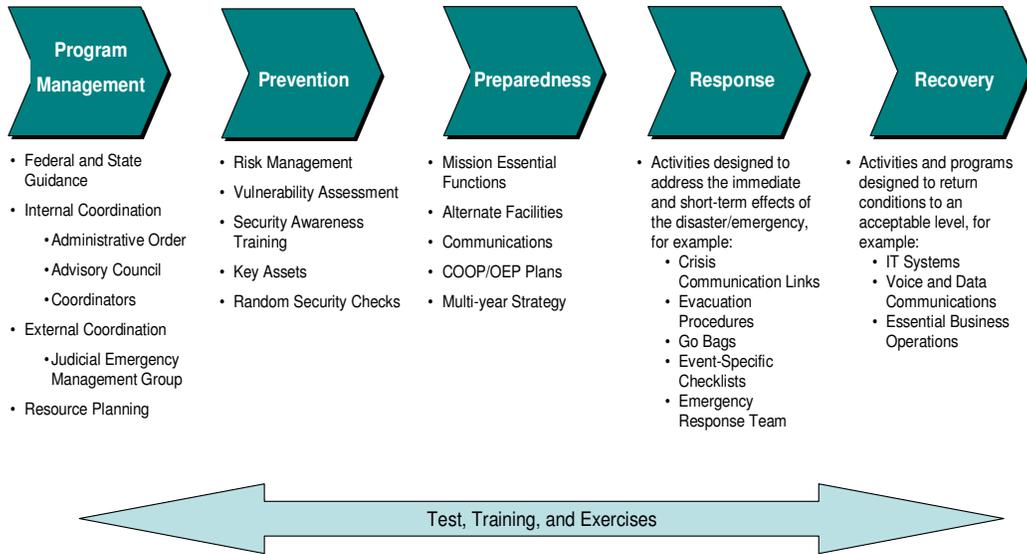
The following illustrates the steps needed for the development of comprehensive security and emergency preparedness programs for state and local courts.

Strategy for a Comprehensive Emergency Preparedness Program

Vision

To institutionalize an approach to emergency preparedness that ensures that Court entities continue to perform their statutory mandates if or when confronted with a broad array of potential operational interruptions.

Emergency Preparedness Program Elements



Note: On the next page the NCSC Best Practices Institute’s report *Emergency Management for Courts*, provides an overview of the subject and briefly introduces best practices.



Best Practices Institute

Emergency Management for Courts



Overview

Emergency management¹ is critical to court performance. For many years, court leaders have been concerned with ensuring the safety of all who use the nation's courthouses. During the 1978 Second National Conference on the Judiciary, participants recognized that "security in the courtroom and in the courthouse has been an increasing problem in recent years" (Friesen, 1978, p. 195). The 1990 *Trial Court Performance Standards* required courts to ensure the safety of their facilities (Commission on Trial Court Performance Standards, 1990). In 1995, the National Association for Court Management produced the *Court Security Guide*, and several states followed with their own security manuals.

This focus on emergency management increased exponentially following the terrorist attacks on September 11, 2001. Since then, the court community has heightened its efforts to address safety issues across the board. For example, the September 2002 *9-11 Summit* (<http://www.9-11summit.org/>) brought together court leaders from across the country to discuss emergency management and pool the knowledge of court professionals who experienced emergencies firsthand. Judicial organizations also responded by offering programs on, creating committees to specifically address, and writing journal and newsletter articles on emergency management. The Best Practices Institute Board also acknowledged the importance of emergency management by designating it a focus area for the Institute in 2002-2003.

References

Commission on Trial Court Performance Standards. (1990). *Trial court performance standards with commentary*. Williamsburg, VA: National Center for State Courts. Also available http://www.ncsconline.org/D_Research/TCPS/Standards/stan_1.2.htm.

¹ The term "emergency management" encompasses all activities related to preventing, planning for, and responding to a crisis situation affecting court operations. See the section "What Does Emergency Management Include?" for more information.

Friesen, Jr., E. C. (1978). Internal organization and procedures of the courts. In T. J. Fetter (Ed.), *State courts: A blueprint for the future* (pp. 179-202). Williamsburg, VA: National Center for State Courts.

National Association for Court Management. (1995). *Court security guide*. Williamsburg, VA: Author.

WHY DEVELOP EMERGENCY MANAGEMENT BEST PRACTICES?

As a result of the increased attention on emergency management, many excellent resources are available to help state and local courts address issues of specific concern to them. The *9-11 Summit* Web site (<http://www.9-11summit.org/>) provides a compendium of materials related to emergency management, including templates for conducting security audits. Given the wealth of information available, some court professionals may be uncertain about where to start in reviewing the effectiveness of their current plans. To assist them, the Best Practices Institute asked five experts to identify a few practices that all courts should consider as first steps to enhance their emergency management efforts — steps that can be taken without the significant expenditure of additional resources.

HOW WERE THE PRACTICES DEVELOPED?

The emergency management practices were drafted by Institute staff (based on themes from conference presentations and resource materials) and vetted by five experts in the area of court safety: Ms. Wendy E. Deer, Counsel to the Deputy Chief Administrative Judge, New York State Office of Court Administration; the Honorable Jonathan Lippman, Chief Administrative Judge, New York Unified Court System; the Honorable Joel D. Medd, District Court Judge, Grand Forks, North Dakota; Mr. Zygmunt A. Pines, Court Administrator of Pennsylvania; and Mr. Steven Steadman, Senior Consultant, Policy Studies, Inc. All of these individuals have been very involved in state and local efforts to address emergency management for courts. The Institute gratefully acknowledges the contributions of these individuals.

WHAT DOES COURT EMERGENCY MANAGEMENT INCLUDE?

The Federal Emergency Management Agency (FEMA) defines an emergency as “any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility’s financial standing or public image (<http://www.fema.gov/pdf/library/bizindst.pdf>, p. 5). FEMA defines emergency management as “the process of preparing for, mitigating, responding to and recovering from an emergency” (<http://www.fema.gov/pdf/library/bizindst.pdf>, p. 6). The emergency management best practices are based on these broad definitions of emergency and emergency planning. Emergency management refers to protecting the court or court system from any event that could threaten its operation – whether the event is an act of man or an act of nature. It encompasses all activities commonly associated with the terms “court security” and “court safety.”

WHAT ARE THE BEST PRACTICES?

The following seven practices, drafted in 2003, are offered as a starting point for courts to review their current emergency management plans. An overview of each practice is presented, followed by examples of how the practice could be or has been implemented. A list of resources for additional information also is provided.

1. ENSURE VISIBLE COURT LEADERSHIP.

The court’s leaders set the tone for effective emergency management. They send the message that planning and practicing for emergencies is the right thing to do — that it is part of the court’s culture. Although they should be involved in all stages of the effort, it is especially important that court leaders be visible at various points in the process to reinforce the importance of the effort and make sure that everyone complies with the resulting plan.

Court leaders also should be visible and accessible during emergencies. To the extent that leaders demonstrate a commitment to address problems and return to business as quickly as possible, staff will be reassured and recovery efforts more systematic and effective.

Examples

- ✓ Court leaders participate in security drills and other efforts to insure safety.
- ✓ Following the September 11, 2001 terrorist attacks on the World Trade Center, Chief Judge Kaye immediately consulted with court leaders and resolved to keep New York’s courts opened. During the next 72 hours, they worked around the clock, touring courthouses, talking with and reassuring court staff, and making alternate arrangements where necessary to keep the courts operating.
- ✓ Following the April 19, 1995 bombing of the Murrah Federal Building, Chief Judge David Russell of the U.S. District Court, Western District of Oklahoma, held a conference with the court’s judges and determined to reopen the court as quickly as possible. In the days that followed, the judges made a concerted effort to keep information flowing to staff and include staff as much as possible in the decision making process. Three days after the attack, the judge convened a staff meeting with psychologists, clergy, and FBI representatives to answer questions and provide support.

Resources

- ✓ “Coping with Disaster.” Chief Judge Judith Kaye, *Judicature*, v. 85 issue 3, pgs. 112-114. (Provides firsthand account of 9-11 disaster from leadership perspective.) <http://www.9-11summit.org/materials9-11/911/acrobat/26/P1LeadingtheCourts/KayeCoping.pdf>
- ✓ “Emergency Management Guide for Business & Industry.” FEMA, p. 6. (Discusses the importance of having management support to create emergency plan.) <http://www.fema.gov/pdf/library/bizindst.pdf>
- ✓ “September 11th: the New York Experience.” Hon. Jonathan Lippman, Conference of State Court Administrators mid-year meeting, November 30, 2001. (Focuses on the leadership and representation of the judicial system within the community during the 9-11 attacks.) <http://www.9-11summit.org/materials9-11/911/acrobat/26/P1LeadingtheCourts/911NYExperience.pdf>

2. SURVEY AND PRIORITIZE EMERGENCY MANAGEMENT NEEDS.

Courthouses are public buildings. Because they must remain open to the public, emergency management issues are complex. There is a balance to strike between ensuring public access and providing a safe and secure environment. Court leaders and staff can strike an appropriate balance and give themselves an advantage by taking time to examine the courthouse (or building designs if the structure is under construction) and to determine potential areas of vulnerabilities. What are the most critical emergency management issues? Which areas should be addressed immediately? Answers to these questions will help court officials develop an effective emergency management plan and to make winning arguments when trying to obtain additional resources.

Examples

- ✓ Courts have asked the United States Marshals Service, local law enforcement, and local universities with programs in law enforcement to conduct security audits of their facilities.
- ✓ Some courts maintain an incident reporting system and database to identify and address specific problem areas. The database also can be helpful in seeking funding.
- ✓ Court employees are good sources of information regarding potential vulnerable areas of the courthouse. Where do they feel safe or not safe? Reaching out to the staff also helps to raise the visibility and importance of emergency management.

RESOURCES

- ✓ “Court Security Manual.” State of Minnesota & Conference of Chief Justices, 1997. (*See security checklist beginning on p. 2-3-1.*) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/MinnesotaCtSecurityManual.pdf>
- ✓ “Court Security Incident Reporting Form.” Minnesota Department of Public Safety, Bureau of Criminal Apprehension, 1993. (*Provides an example of an incident reporting form.*) <http://www.dps.state.mn.us/bca/Forms/Documents/court-incid.pdf>

- ✓ “Measure 1.2.1: Courthouse Security Audit.” Commission on Trial Court Performance Standards, 1995. (*Includes National Sheriffs’ Association Physical Security Checklist.*) http://www.ncsconline.org/D_Research/TCPs/Standards/stan_1.2.htm

- ✓ United States Marshals Service. (*Includes address and telephone numbers of district offices.*) <http://www.usdoj.gov/marshals/usmsofc.html>

3. CREATE AND PRACTICE AN EMERGENCY RESPONSE PLAN.

It is important to have a plan in place in anticipation of various emergency situations (e.g., breach of courthouse security, natural disaster, electrical outage, bomb threat, or explosion). A court emergency management committee consisting of court leadership, the court’s automation specialist, law enforcement, the facilities manager, and other interested parties such as representatives of the bar and members of the public is necessary to determine the critical emergency management issues to address in the plan and the most effective and least costly responses.

An essential task for the committee is to identify who will make key decisions in the event of a crisis. This will avoid turf battles or delayed or inconsistent responses because the lines of responsibility are blurred.

Creating the response plan is necessary but not sufficient. Regularly communicating with staff, providing training, conducting drills, and testing equipment are also vital components of an effective plan.

Examples

- ✓ Some states have an emergency management manual with templates to help local courts create their plans. See, for example, Florida’s template for Continuity of Operations Plan on p. 62 of “Keep the Courts Open” and New York’s “Facility Emergency Preparedness and Response Plan,” both cited in resources below. (If your state has a template to include in the resources cited below, please forward to pcasey@ncsc.dni.us.)
- ✓ In addition to the overall plan, some courts create mini-documents customized for specific depart-

ments and/or specific crises (e.g., fire, flood, electrical outage). These smaller documents include the basic information each employee needs to know in the event of an emergency and are more user-friendly than the entire plan. See, for example, New York's Employee Evacuation Checklist in Appendix C of "Emergency Preparedness and Response Planning Manual" cited in resources below.

- ✓ Courts conduct mock disaster drills to identify and address problems with the plan and to maintain court staff interest in the plan. See, for example, New York's Evacuation Drill Report in Appendix F of "Emergency Preparedness and Response Planning Manual" cited in resources below.
- ✓ If time and resources are a problem, consider training staff a little at a time. One court developed materials specific to the needs of the custodial staff and reviewed and discussed the information with the staff. It only took about 15 minutes, and the staff was very appreciative of, and later used, the information.

RESOURCES

- ✓ "Contingency Planning: COOP Self-Assessment Guide & Checklist." Federal Executive Branch. (Provides a checklist that can be used to develop a contingency plan. Includes checklists for essential functions, authorities & delegations, alternative facilities, communications, program management, and testing exercises.) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/SelfAssessGuideChecklist.pdf>
- ✓ "Court Security Manual." State of Minnesota Conference of Chief Judges. (A statewide resource for enhancing court security. See courthouse contingency plans beginning on p. 2-4-1 and training outlines beginning on p. 12-1-1.) <http://www.9-11summit.org/materials9-11/911/acrobat/26/C6NewThreats/MinnesotaCtSecurityManual.pdf>
- ✓ "Emergency Preparedness and Response Planning Manual with Appendices." New York State Unified Court System, March 2003. (A statewide planning guide that identifies tasks and issues courts need to address to be prepared for a broad range of emergencies.) <http://www.9-11summit.org/materials9-11/911/acrobat/26/manual1.pdf> and <http://www.9-11summit.org/materials9-11/911/acrobat/26/manual1-append.pdf>
- ✓ "Facility Emergency Preparedness and Response Plan." New York State Unified Court System, March 2003. (Provides a template for each court to prepare a response plan in the event of an emergency.) <http://www.9-11summit.org/materials9-11/911/acrobat/26/template.pdf>
- ✓ "Keep the Courts Open." Final report of the Florida Supreme Court Workgroup on Emergency Preparedness, March 28, 2002. (A statewide resource for courts to plan for emergencies. See p. 62 for COOP template.) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/FloridaFinalReport.pdf>
- ✓ "Occupant Emergency Program Guide." U.S. General Services Administration Public Buildings Service, Federal Protective Service, March 2002. (Discusses essential components of an occupant emergency plan.) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/GSAOccupantEmergencyProgram.pdf>
- ✓ "Wisconsin Courthouse Security Resource Center." The Wisconsin Sheriff's and Deputy Sheriff's Association, U.S. Marshal's Office of the Western District of Wisconsin, Director of State Courts, Office of the Chief Justice of the Wisconsin Supreme Court, Fox Valley Technical College, 2000. (The Center provides training, research, and technical assistance related to security. The document includes Chapter 7 from the Wisconsin Courthouse Security Manual that discusses creating contingency safety and security plans.) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/Wisconsinexcerpt.pdf>

4. GET A SEAT AT THE TABLE.

Make sure that the court or court system has a representative present in city, county, or state emergency

management meetings. Courts generally have not actively engaged in reaching out to other government agencies (and some agencies have not been open to court participation) to address emergency management issues. As a consequence, courts may find themselves at the bottom of a long list of priorities when city, county, and state emergency recovery plans are enacted. It is important to understand which agencies are in charge of emergency preparedness in your jurisdiction and to have a court staff person with appropriate decision authority contact and meet with the individuals in charge. If there are no regular communications among emergency management officials in the jurisdiction, the court can be an advocate for creating an ad hoc committee to coordinate efforts across the jurisdiction.

Examples

- ✓ The U.S. District Court, Northern District of West Virginia, found a very receptive emergency management network when the chief judge began calling emergency responders in the community. As a result, the court was part of a mock drill, and local and state officials expressed gratitude to the court for taking a leadership role.
- ✓ State officials in Florida made contacts with state emergency planning agencies to facilitate contacts at the local level. In addition, the state office named an emergency coordinating officer in each circuit and appellate court district whose primary responsibility is to connect with the existing emergency management network in the community.

Resources

- ✓ "Communication is Key in Court Security." Amanda Murer, Report on Trends in the State Courts, National Center for State Courts, 2002. (*Touches on the importance of communication with others in community when making a security plan. Also gives ideas of how to improve court security plan without monetary support.*) http://www.ncsconline.org/D_KIS/Trends/Trends02MainPage.html
- ✓ "Emergency Management Guide for Business & Industry." FEMA, pgs. 39-40. (*Discusses emergency planning with other community agencies.*) <http://www.fema.gov/pdf/library/bizindst.pdf>

- ✓ Homeland Security Contact List. Whitehouse Web site: <http://www.whitehouse.gov/homeland/contactmap.html>
- ✓ "Keep the Courts Open." Final report of the Florida Supreme Court Workgroup on Emergency Preparedness, March 28, 2002. (*Discusses the importance of communication and cooperation in planning for responses to threats and emergencies.*) <http://www.9-11summit.org/materials911/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/FloridaFinalReport.pdf>
- ✓ Office of Domestic Preparedness, U.S. Department of Justice. <http://www.ojp.usdoj.gov/odp>. (*Web site from the DOJ to help first responders deal with incidents of terrorism and weapons of mass destruction.*)
- ✓ State Offices and Agencies of Emergency Management. (*Includes state emergency manager's email address.*) <http://www.fema.gov/fema/statedr.shtm>

5. DEVELOP A PLAN TO COMMUNICATE INTERNALLY.

The court should develop alternative plans for communicating with staff in the event of an emergency. Because different communication systems may fail depending on the emergency, it is important to plan for various scenarios (e.g., phone lines down, satellite connections blocked, internet unavailable). During an emergency, some type of central command communication system is critical. Conflicting messages from different sources will increase anxiety and slow efforts to address an emergency.

Examples

- ✓ Designated court officials maintain an emergency contact list of all employees. Contact information includes home address, phone number, beeper, cell number, and email address, as appropriate. Managers and supervisors have a list of emergency contact numbers for each staff person in their respective office or department. A copy of the list is kept in the manager's office and home.

- ✓ “Phone trees” are an example of a low-cost method to keep court staff informed during the initial period following an emergency if the court’s regular communication system is unavailable.
- ✓ Designating a central place to gather following an emergency helps court officials determine who is missing.
- ✓ Some courts provide staff a laminated “emergency card” to carry in a wallet, purse, or glove compartment. The card lists phone numbers each staff person should call in the event of an emergency, the court’s Web site, and television and radio stations that broadcast information about the court during an emergency. The cards are updated periodically to keep them current.

Resources

- ✓ Continuity of Operations Plan (COOP) Plan Coordination Draft.” Federal Executive Branch, August 13, 2002. (*See Annex L: Emergency Notification.*) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/ContinuityOperationsPlanFEbranch.pdf>
- ✓ “Emergency Management Guide for Business & Industry.” FEMA, pgs. 31-32. (*Discusses emergency communications considerations.*) <http://www.fema.gov/pdf/library/bizindst.pdf>
- ✓ “Emergency Preparedness and Recovery Procedures Manual.” 11th Judicial Circuit of Florida, Administrative Office of Courts, July 31, 2002. (*See section one on communications. Includes description of telephone tree.*) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/EmergencyProceduresRecoveryManual.pdf>
- ✓ “Keep the Courts Open.” Final report of the Florida Supreme Court Workgroup on Emergency Preparedness, March 28, 2002. (*See p. 76 for employee notification procedures during an emergency. Appendices E and F provide employee profile forms and an emergency contact log to use during a crisis.*) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/FloridaFinalReport.pdf>

- ✓ “You Can Help Keep the Courthouse Safe” & “What is Suspicious.” Sample handouts provided by Tina Rowe for 9-11 Summit panel on Emergency Preparedness Planning: A Workshop, 2002. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/RoweSampleHandout.pdf>

6. DEVELOP A PLAN TO COMMUNICATE EXTERNALLY.

Depending on the emergency, courts may have to contact numerous other individuals who are or could be affected by the crisis (e.g., attorneys, litigants, witnesses, jurors, other justice system and human service agency staff who work with the court, the general public). Courts should prepare a list of individuals who might be affected by a court emergency and determine the best way to communicate with them (e.g., work through the local bar to send a message to attorneys, use the court’s Web site to provide information to the public).

As is the case for internal communications, it is critical that external court communications be consistent and accurate. The court’s leadership should inform the communications point person what information is communicated, when, and to whom. Messages should be operationally simple (e.g., how to contact the court, whether cases will be heard, alternative locations for conducting business) and provide a number or Web site to obtain more specific information. Frequent updates as information is obtained will lessen the public’s anxiety and facilitate the recovery process during an emergency.

Examples

- ✓ Contact information of individuals who will (1) provide information and feedback to the court during an emergency and (2) help the court get its message out to affected groups is maintained by the court manager and communications point person and regularly updated.
- ✓ During the initial hours and days of a community-wide emergency, court information may not be a priority for media outlets to provide. Courts in this position have sought other means to communicate such as paying for an announcement in

local newspapers, using the court's Web site to provide information, maintaining an information hotline at the court, or providing a toll-free number for court information, installing internet phone lines, and asking other branches of government that may have better access to the media to include information about the courts in their briefings.

- ✓ During a crisis in Florida, the Supreme Court's communications officer and marshal work in the state's Emergency Operations Center. The Center maintains toll-free numbers for the public seeking information. Calls requesting court information are routed to the court officers.
- ✓ In Puerto Rico, the state court administrator calls the bar president, the attorney general, and the chief of police to provide information regarding the operations of the courts. These officials subsequently inform their respective staff.

Resources

- ✓ "Emergency Management Guide for Business & Industry." FEMA, pgs. 41-41. (*Discusses emergency communications with the public.*) <http://www.fema.gov/pdf/library/bizindst.pdf>
- ✓ "The Administration of Justice Under Emergency Conditions: Lessons Following the Attack on the World Trade Center." Oren Root, Vera Institute of Justice, January 2002. (*See recommendations regarding communications on pages 25-26.*) <http://www.9-11summit.org/materials/9/11/911/acrobat/26/CITheAftermath/VeraInstituteLessonsFollowingAttack.pdf>

7. DON'T LET RESOURCES PREVENT PLANNING.

Emergency management is a core court activity. Courts cannot afford to wait until extra resources become available before they start planning. Expensive new technology and security consultants are not necessary to begin integrating the importance of emergency management into the court's culture.

Courts can begin with low-cost planning activities and explore opportunities for additional resources as the planning process unfolds. As courts reach out to other community and government entities to create

an effective plan, they may learn of expertise that resides in the community and funding sources they do not normally access.

Courts also should include stakeholders and members of the public on emergency planning committees. This not only insures that the public's voice is included in the plan but also creates community advocates for the plan. The court's request for funding to implement the plan is likely to be more effective coming from a member of the public. Members of the public arguing for funding to safeguard the courthouse reinforces the idea that the funds are needed for the protection of the public as well as for judges and court staff.

Examples

- ✓ *9-11 Summit* participants reported that costs associated with planning were minimal. In addition, they noted that some improvements, such as developing or modifying outdated policies and procedures and compiling emergency contact information for each employee, also could be accomplished with limited resources. Police Commissioner Raymond Kelly of New York City suggested giving all court staff a kit with a whistle, mask, and flashlight — low-cost items that could be very helpful in a number of emergency situations.
- ✓ The Wisconsin Courthouse Security Training Program was accomplished through the joint efforts of the Office of the Chief Justice, Director of State Courts Office, Wisconsin Sheriff's and Deputy Sheriff's Association, the U.S. Marshal's Office for the Western District of Wisconsin, the Wisconsin Office of Justice Assistance, and the Fox Valley Technical College. With the help of their law enforcement partners, the Wisconsin Supreme Court obtained grant funds from the Office of Justice Assistance, and the Technical College helped develop, deliver, and evaluate a "train the trainers" curriculum for 400 county-level leaders across the state. Prior to this effort, the court had not participated in such a comprehensive partnership. New skills and resources were developed using this cooperative model.

- ✓ Training and technical assistance in emergency management may be available from local, state or federal sources outside of the judicial branch. For example, one or more community agencies may offer emergency management training and would be willing to have court representatives participate. Expertise in emergency management also may be available through local law enforcement or local colleges that offer programs in law enforcement and emergency management. These local agencies also may have access to additional resources through their wider emergency management networks. For example, the Office for Domestic Preparedness (ODP), Department of Justice, provides funds to each state to address specific equipment, training, and technical assistance needs to help state and local jurisdictions better respond to incidents of domestic terrorism. ODP and the Naval Postgraduate School also offer a Masters Degree Program in Homeland Defense and Security for government employees. Individuals can determine if they are eligible for the program by visiting the Homeland Security Leadership Development Web site at www.hsld.org.

Resources

- ✓ “Homeland Security Exercise and Evaluation Program, Volume I: Overview and Doctrine.” Office for Domestic Preparedness, U.S. Department of Homeland Security, March 2003. (*Chapter 1 provides a description of the State Homeland Security Grant Program.*) <http://www.ojp.usdoj.gov/odp/docs/HSEEPv1.pdf>
- ✓ “Wisconsin Courthouse Security Resource Center.” The Wisconsin Sheriff’s and Deputy Sheriff’s Association, U.S. Marshal’s Office of the Western District of Wisconsin, Director of State Courts, Office of the Chief Justice of the Wisconsin Supreme Court, Fox Valley Technical College, 2000. (*Example of a partnership that provides training, research, and technical assistance related to court security.*) <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/Wisconsinexcerpt.pdf>
- ✓ “Enduring Values in Changing Times.” Chief Justice Shirley S. Abrahamson, Annual Meeting of the Wisconsin Judicial Conference, 2002 State of the Judiciary — October 16, 2002, p. 8. (*Brief description of growth of Wisconsin Courthouse Training Program.*) <http://www.wicourts.gov/media/pdf/02stjud%2Dchieforg.pdf>

About the Best Practices Institute

The Best Practices Institute identifies and promotes practices that enhance the effective administration of justice. The Institute was created at the direction of the boards of the Conference of Chief Justices, the Conference of State Court Administrators, and the National Center for State Courts following the 1999 National Conference on Public Trust and Confidence in the Justice System. During the conference, participants repeatedly voiced the need for a national effort to identify and champion best practices from across the country as part of a broad strategy to improve court performance and better serve the public.

The Institute was inaugurated in the fall of 2000. Its work is guided by an advisory board of chief jus-

tices, state court administrators, a court manager, a presiding judge, and a legal scholar. The intent of the Institute is to provide a central resource to which the 50 state court systems and their state trial courts can turn to obtain the field’s best thinking across the spectrum of judicial administration. For more information, please visit the Institute’s Web site at http://www.ncsconline.org/Projects_Initiatives/BPI/index.htm.



Chapter 1: Standard Operating Procedures

The cornerstone for any effective program of court security and personal safety is a comprehensive and cohesive set of standard operating procedures. The establishment of such standard operating procedures was ranked by court administrators in a 2004 survey conducted by the National Association for Court Management (NACM) as the first important step in a court security program.

There are two crucial factors to consider with respect to standard operating procedures. The first factor is simply that such procedures usually do exist. This means that those in authority have given these matters proper thought, that concepts of best procedures have been taken into account, and that an effort has been made for consistency in security matters throughout the system. The second factor to consider is how such practices become a living reality and are practiced inside court buildings. Thus, policies and procedures must not only be promulgated, but must also be the subject of a rigorous training regimen and ongoing communication efforts. Everyone who works in a court building has the potential to enhance the safety and security of his or her work environment materially, to be the eyes and ears of a workforce constantly alert to risks and threats. Judges and court staffs that have been well trained on well-publicized policies and procedures provide the best means for this function to be effectively discharged.

Without standard operating procedures, those in court leadership positions have no basis to resolve their courts' safety and security concerns. With a solid set of operating procedures, court leaders can systematically address such issues and effectively minimize risks inherent in court operations.

The Committee has identified ten topic areas requiring standard operating procedures. These topics were from standards and recommendations contained in material (*e.g.*, court security manuals, directives, policies, rules) from the following states and organizations: Alabama, American University, Arizona, California, Delaware, Florida, Michigan, National Association for Court Management (NACM), National Sheriffs' Association, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Tennessee, Utah, Washington, and Wisconsin.

In this chapter, specific standard operating procedures are set forth or referenced for each of the ten topics. In some cases, information for the topic is summarized here, with more information on the topic contained in another, cross-referenced chapter. (See topics 2, 3, 4, 6, 7, and 10.) Topic 5 (Physical Security) encompasses a wealth of suggested standard procedures in a great variety of physical and operational areas, which are summarized below. The procedures themselves are set forth in Appendix A of this handbook.

Topic 1: Leadership/Commitment/The Security Plan

Critical to the security endeavor is visible commitment from state and local judicial leadership (chief justice, presiding/chief judge, court administrator) to stress the importance and necessity of protecting the public, court personnel, judicial records, and court facilities. Court security requires careful planning and continual concerted action. It is important to ensure active commitment to court security by requiring (*e.g.*, by order or directive) written security plans that systematically address the following security needs:

- Standard operating procedures
- Emergency procedures/protocols
- Continuity of operations plans (COOP)
- Governance of shared facilities
- Disaster recovery
- Communications protocols
- Employee training
- Equipment testing

Security plan implementation in states varies. Some state courts identify security measures as mandatory standards; others refer to them as guidelines.

Topic 2: Collaboration and Coordination

Collaboration and coordination are key ingredients in any safety and security program. This applies from both an internal and external perspective. Internally, it is important to (a) establish within each judicial district a standing committee on court security, chaired by the supervising judge and including major stakeholders such as court administrators, local law enforcement officers, executive branch officials, facility

managers, and officials responsible for funding court security; (b) establish an identifiable and distinct position-holder (a security administrator or coordinator) within each facility who will serve as a point of contact and assume responsibility for the facility's security needs, implementation of security procedures, coordination of activities in an emergency, and collaboration with the local court security committee; and (c) create a state level security administrator position to provide direction, guidance, and oversight for security of the state's courts.

Externally, it is important for the court to establish formal, routine alliances or partnerships with local and state security entities (*e.g.*, state homeland security office), officials, and law enforcement to ensure effective communication and collaboration to address the judiciary's distinct security needs. External partnerships are discussed in more detail in Chapter 9 of this handbook, "Resources and Partnerships," Essential Element 9.

A clear command structure – the designation of who is in charge – is critical to quick action. A designated person in each facility should be authorized to declare an emergency and to make decisions in the event of an emergency, especially if a facility is shared with multiple courts or non-judicial departments. There should be a clear unity of command structure to identify who specifically is responsible for securing a building. If the court cannot reach agreement with a facility's non-judicial occupants, the court should define and make adequate provisions to control its space.

Topic 3: Self-Assessment (Audits)

There are many significant ways to minimize the risks inherent in court operations. A court can make significant progress in minimizing risks by conducting its own security audit. A security self-audit entails a comprehensive and systematic effort on the part of court leadership to identify security risks within and around the courthouse. These security audits can be conducted at little or no cost by court staff and/or sheriff's deputies. Armed with information obtained through such audits, courts can prioritize the risks and then develop plans and budgets to correct security deficiencies and make courthouses safer places in which to work and visit.

Security self-assessments are discussed in detail in Chapter 2, “The Self-Audit,” Essential Element 2.

Topic 4: Security Personnel (Staffing)

The facility should be adequately staffed with trained and properly assigned security personnel to monitor the facility, operate security equipment effectively, and respond to emergency/security needs at all times. For example, California recently adopted guidelines for the funding and staffing of court security personnel based on the number of filings and judgeships in each trial court. The recommended ratios are one sergeant position for every 12 nonsupervisory positions and 1.7 deputy sheriffs for each judicial position.

A court facility should identify the important areas where security officers are needed and allocate sufficient staff with clearly designated responsibilities to those areas. Only security personnel who are properly trained and qualified in court security (including the use of force and weapons) should be assigned. Some states use civilian or contract personnel. California is authorized by statute to use civilian court attendants in non-criminal cases to allow better use of security resources where they are needed most. Such use, thus far, has reportedly been very limited. The preferred approach seems to be the use of uniformed officers trained in courthouse security and use of weapons (*e.g.*, Washington), but such an approach may be two to three times more costly than the privatization route. Use of private security or contract vendors may lower security costs but may also pose some disadvantages (*e.g.*, restrictions on ability to make arrest, difficulty in coordinating with local law enforcement). If a court contracts for security services, all security personnel should be subject to security clearance and be properly trained/certified in court security. Law officers in court for other reasons should not be considered a component of a court's security system.

Topic 5: Physical Security (Perimeter, entry, and interior areas)

Standard operating procedures are needed in all of the following physical and operational areas:

A. Perimeter Security

1. Parking areas
2. Grounds (lighting, visibility, protective distance)
3. Exterior of buildings (potential access routes)
4. Surveillance (patrols, daily inspections)
5. Equipment (alarms, surveillance)
6. Loading docks

B. Entrance Security – Access to the Facility

1. Limited access (single point of entry concept)
2. Controlled access (screening post)
3. Screening of mail and deliveries
4. Personnel
5. ID and access control procedures
6. After-hours operations
7. Weapons policy
8. Other policy considerations: contraband, use of force
9. Custodial services
10. Vendors/independent contractors

C. Interior Security — Generally

1. Circulation zones
2. Locking devices: utility and environmental controls
3. Identification and monitoring procedures
4. Security equipment
5. Security personnel (training and safety)
6. Internal communications (within the facility)
7. Prisoner transport/holding areas
8. Building/personnel profiles
9. Daily inspections/sweeps
10. Personal security planning

D. The Courtroom

E. High-risk Proceedings and Populations

F. Administrative Offices

G. Judicial Chambers

H. Roof Exits, Hallways, and Stairwells

Recommended standard operating procedures for all of the above physical and operational areas are found in Appendix A.

Topic 6: Incident Reporting and Recording

Security incidents should be properly and carefully defined, and security breaches should be immediately reported to law enforcement or a designated court security officer. Security incidents and breaches should be promptly documented on an easy-to-use standardized form and given to the facility's security manager for prompt assessment. Information obtained from security incident/breach reporting should be tabulated and regularly assessed by the local court security committee to determine how security can be improved. Security incident reports should be treated as confidential, and distribution should be carefully controlled.

Incident reporting is discussed in detail in Chapter 6, “Incident Reporting,” which covers Essential Element 6.

Topic 7: Records and Information

Courts should create and enforce record retention and destruction policies. All court records and files should be safely secured and stored to protect them from theft, misuse, damage, or destruction. Information stored in computer systems should be backed up and then stored off-site to enable prompt retrieval of information. Courts should take measures to insulate their computer networks from infiltration or sabotage. There should be separate and secure storage for exhibits, including firearms, ammunition, currency, etc. Courts should identify resources that will be able to provide immediate assistance in salvaging and restoring court records in the event of an emergency. Access to court records and confidential information such as medical and personnel records should be restricted and monitored.

Storage and retrieval of essential information is discussed in detail in Chapter 4, “Disaster Recovery – Essential Elements of a Plan,” which covers Essential Element 4.

Topic 8: Education and Enforcement

Routine mandatory security training should be required for all facility occupants. A core curriculum is recommended. There should be instruction on evacuation, emergency, and lock-down procedures. There should be periodic, unannounced mock security drills for all who work in the court facility. Information should be provided to

judges and staff about how they can enhance safety in their personal lives, including the development of family emergency plans, which is strongly recommended. New York and Pennsylvania, for example, provide a *Judicial Threats Handbook* to every judge. New York's security task force report recommended that a list of telephone numbers and crucial first steps should be given to every judge in a convenient, portable form (e.g., wallet-sized card). The report recommended other considerations to provide judges with prompt communication capabilities, such as portable home duress alarms and cell phones with global positioning capacity.

Law enforcement and/or court security officers who work in the court facility must be adequately trained and certified in the skills and performance standards required to execute their court security roles and responsibilities. Such training should include instruction in the transportation and restraint of prisoners, court facility security procedures, use of force, dealing with the public, etc.

Security procedures and protocols should apply to all who work in or visit the court facility and be strictly enforced. Effective court security requires 100percent compliance. Security is a collective and individual responsibility that affects everyone. Enforcement of court security procedures is the responsibility of management (presiding/chief judges, judges, court administrators, and facility managers). Court staff should be clearly advised that failure to comply with a facility's security procedures and protocols may be grounds for disciplinary action. Security personnel should be consulted and security procedures should be followed when employees are terminated.

Topic 9: Communication

Court staffs and judges should know what is expected of them at all times. Clear and simple security information should be provided. For example, information can be provided through the posting and dissemination of security directives and rules; security manuals and handbooks; periodic security bulletins, announcements, newsletters, emails, etc.; and wallet-sized laminated cards containing important basic information (such as telephone numbers, courthouse Web site, emergency contacts, and emergency procedures).

Topic 10: Funding

The cost of security should be included as an essential business expense in a court's annual budget. *Courts must seek adequate funding to support their security needs, including physical infrastructure, operational enhancements, human resources, and other components of an effective and comprehensive court security program.* Many security measures (such as leadership, security committees, security protocols, and communication) are achievable at little or no cost. For costly measures such as security equipment and security staff, courts can seek to augment their budgets on an incremental basis. California recently adopted guidelines for funding and staffing of court security personnel based on the number of filings and judgeships in each trial court. The recommended ratios are one sergeant position for every 12 non-supervisory positions and 1.7 deputy sheriffs for each judicial position. A recent report indicated that California allocated 16 percent of its court budget for court security. In addition to the number of filings, other factors, such as building design and specific functions performed within the building, will affect the calculation of security staffing levels.

Funding is discussed in more detail in Chapter 8, “Security Equipment and Costs,” which covers Element 8. Also see Chapter 9 of this handbook, “Resources and Partnerships,” which covers Element 9.

References/Resources

Fautsko, Timothy F. *Courthouse Safety Training: for the Courts of Appeal of Maryland, Dept. of Emergency Preparedness and Court Security.* Denver, CO: National Center for State Courts. 2009.

< <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=151>>.

New York State Unified Court System. “The Task Force on Court Security – Report to the Chief Judge and Chief Administrative Judge. October, 2005.

<http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf>.

Superior Court of California, County of San Mateo. “1999 Final Report: Courthouse Security.” *Security and the Courts Resource Guide.* 1999.

<<http://www.sanmateocourt.org/director.php?filename=/grandjury/1999/99courthouse.html>>.

“Table of Contents.” *Justice System Journal*. Vol. 28, No. 1. 2007.

http://www.ncsconline.org/D_Comm/Projects/JSJindex/JSJ_TOC/Vol28_1/vol28_1.html.

Wisconsin Supreme Court. “SCR Chapter 70: Rules of Judicial Administration Rule 70.39.” Dec 9, 2004. <

<http://www.wicourts.gov/sc/scrule/DisplayDocument.html?content=html&seqNo=1072>>.

Chapter 2: The Self-Audit

The Nature and Purpose of a Court Security Self-Audit

Operating a courthouse is by its very nature a risky business. Day in and day out, courthouses are visited by a large number of disgruntled, even lawbreaking citizens. In addition, courthouses are seen as important symbolic targets for individuals who may want to cause mischief or inflict terror. Given these risks, court leaders and security officials need tools to help them provide a reasonably safe environment for those who work in and visit their courthouses each day.

There are many significant ways to minimize the risks inherent in court operations. Some are costly; others are not. However, before risks can be minimized, they need to be identified with specificity. Optimally, court security experts or organizations can be consulted to perform a comprehensive assessment of courthouse security risks. Yet in times of tight budgets, funds might not be available for courts to retain outside experts. This should not, in itself, be a deterrent to security assessment, since the court can make significant progress in minimizing risks by conducting a security self-audit.

A security self-audit is a comprehensive and systematic effort on the part of court leadership and security officials to identify security risks around and within the courthouse. These self-audits can be conducted at little or no cost by court administration and/or law enforcement officers. Armed with information obtained through such audits, court officials and security providers can prioritize risks to their court and then develop plans and request budgets to correct security deficiencies and make their courthouse a safer place.

Topics to Cover in a Security Self-Audit

There are two categories of topics to consider in a security self-audit: tangible and intangible. Tangible topics are items that cost money and are essential for courthouse security: the physical plant, equipment, technology, and personnel. –. Intangible topics include items that generally cost little or no money but are equally essential for effective courthouse security: operating policies and procedures, training, and communication. .

Tangible topics encompass both the exterior and interior of courthouses. Items relating to courthouse exteriors may include secure parking for judges and staff; adequate lighting around

the courthouse perimeter; no shrubbery where dangerous items can be secreted; ground-floor windows that are secure from breaking and entering; doors that are invulnerable to vehicular assault; and a comprehensive intrusion alarm system.

Items in courthouse interiors may include a screening station with magnetometers, x-ray machines, and hand wands that will prevent people from bringing weapons or other dangerous items into the building; armed sheriff's deputies not only staffing the screening station but patrolling lobbies and hallways; a command and control center that monitors a system of closed circuit televisions (CCTVs) with cameras located in such areas as courtrooms, lobbies, and hallways; duress alarms in place at the bench and staff work areas in each courtroom, all judges' chambers, and all work stations behind every public counter; and circulation zones that properly separate public from private areas. These items provide just a sampling of the tangible issues a comprehensive security self-audit will cover.

In terms of intangible items, the self-audit should assess the existence and the content of policies prohibiting or regulating guns and other contraband being brought into the courthouse; critical incident plans in the event of a shooting, bomb threat, hostage situation, or when an irate or disruptive person is on the premises; protocols for documenting and evaluating security incidents; policies governing transport and control of in-custody defendants; policies for conducting background clearance checks and supervising vendors and cleaning crews inside the courthouse; specific procedures for weapons screening; and policies to control after-hours access to the courthouse as well as to limit access to secure areas within the courthouse during business hours. In addition to the policies and procedures mentioned above, other questions to ask about intangibles in the course of a self-audit include the following:

- Are judges, court staff, and law enforcement officials adequately trained to handle court security problems?
- Has the court established an appropriate governance structure (*e.g.*, a court security committee) by which responsibility is clearly assigned for identifying, analyzing, and remediating security issues on a comprehensive and ongoing basis?
- Is there a strategic plan in place for paying continuing and systematic attention to security matters?

How to Conduct a Security Self-Audit

A security self-audit should be conducted based on accepted court security policies and procedures and in cooperation with the court's security committee, which will oversee the successful conduct of the audit and ensure proper remedial steps are taken to correct problems the self-audit uncovers. If court security policies and procedures and/or a security committee have not been established, contemplation of a self-audit provides a good opportunity to establish both. Typically, courthouse security committees are chaired by the presiding or other designated judge and are staffed by the court administrator or building facilities manager. Committee membership should include judges, court staff, sheriff's representative or other law enforcement personnel responsible for court security, first responders to courthouse emergencies, county administrative personnel (including those responsible for building maintenance), and other major tenants and courthouse users, such as district attorneys, bar representatives, etc.

Once established, the courthouse security committee ("Security Committee") should assign responsibility for conducting the self-audit to a small team consisting of the court administrator or facilities manager (or a designee) and a representative of the sheriff or other law enforcement agency providing security services to the courthouse. The Security Committee should review the tools and methodology to be used for the self-audit, assign a timeframe for conducting and completing the audit, review the results of the audit, and develop a budget and plan for implementing corrective actions.

Tools and Methodology for the Self-Audit

Conducting a self-audit will require the use of an assessment form or check list (see "References/Resources" at end of chapter) that reflects the court's security policies and procedures. Besides the National Center for State Courts, organizations such as the National Sheriffs Association and the United States Marshals Service have developed good prototypes of these checklists. California, Kansas, Minnesota, Montana, and Wisconsin have adopted and utilized their own versions of these prototypes. Any national organization that has a demonstrated interest in court security can assist a court in selecting a checklist that is appropriate.

An effective courthouse security assessment form or checklist contains a comprehensive set of elements, usually in question format, relating to security in and around a courthouse.

Questions on the checklists are typically organized around broad topic areas. For example, California's checklist is grouped around administrative issues (policies and procedures); perimeter (parking); building exterior (access); building interior (equipment); building interior (public areas); building interior (restricted areas); and security staff. There should be a strong correlation among the items on a checklist. The standard operating procedures for this topic are set forth in Appendix A. A comprehensive checklist should encompass all of these areas and would be a method for determining the extent to which a court has these standard operating procedures in place.

The checklist will ask questions about tangible as well as intangible matters. The following are examples in the tangible category: Are parking areas safe? Are street-level windows locked or secured? Is there shrubbery around the courthouse that can be used for secreting weapons or other dangerous items? Is there a security entry screening station at each public entrance and is it staffed properly? If so, does the entry screening station include a walk-through magnetometer, x-ray machine, and a wand? How many armed law enforcement officers operate the screening station? Is there a duress alarm at every station behind every public counter?

The following are examples in the intangible category: Does the court have current policies and procedures on courthouse security? Does the court have protocols that address courtroom violence, hostage situations, fires, or evacuation of individuals in case of emergency? Are there procedures in place to identify and dispose of suspicious vehicles parked near the courthouse?

The checklist will typically include space for specific answers (Yes or No), as well as space for brief comments or more expansive descriptions. The form also includes the date, name, position/title, and signature of the individual(s) conducting the audit.

There are two primary techniques to use in the course of conducting the self-audit. The most obvious technique is simply to walk around the exterior and interior of the courthouse to make direct observations. Much of what is in place or is missing that comprises effective courthouse security may be visible to the naked eye. These observations can also provide good opportunities to conduct tests where applicable. Such items as intrusion and duress alarms can be tested to see if they are in proper working order. Doors that should be locked can be tested to make sure they are in fact locked.

The second technique for conducting the audit is to interview those who work in the courthouse every day. These individuals are truly the eyes and ears of courthouse security, and they may reveal information in an interview or focus group that cannot be readily observed, including specific security concerns. For example, some employees may say they cannot hear the public address system in the event of an emergency. Some may report that doors that are supposed to be locked are often kept pegged open.

Interviews can also reveal how familiar courthouse employees are with security policies and procedures. It is particularly important to interview frontline employees, those who deal directly with the public, on the phone, at the front counter, in an office, or inside the courtroom. If threats have been made, these are the employees who are most likely to have experienced them. It may also be useful to conduct these interviews through focus groups composed of frontline staff. These focus groups often serve to get the conversation flowing freely, uncovering useful information.

Evaluating the Results of a Self-Audit

Once the self-audit is completed and the assessment form is filled out, it will be necessary to evaluate the results and to determine remedial action. To some extent, a good assessment checklist will produce results that are relatively easy to interpret, thereby identifying what remedial action can be promptly taken. If the answer to the question about shrubbery is “yes,” an obvious remedial action would be to trim back the shrubbery.

With respect to many of the self-audit items, evaluating the results and recommending remedial action may be more complicated and require more thought. The self-audit may reveal a security deficiency but may not necessarily provide guidance on how to cure the deficiency. Besides accepted policies and procedures, security standards or guidelines may be necessary to help a court determine what steps are needed in order to provide a reasonable level of safety to those who work in or visit the courthouse. For example, the survey may indicate the courthouse does not have CCTV coverage, but will not identify how to prioritize the location of CCTV cameras, nor will it reveal what the operational features of a CCTV system should be.

The Standard Operating Procedures set forth in Chapter 1, particularly Topic 5, “Physical Security,” prescribe much of what needs to be in place in terms of courthouse security. A few national organizations have developed sets of best practices that describe what is needed to

provide a reasonable security level with respect to virtually all the topics that will be covered in the self-audit. To address the concern that full implementation of recommended best practices in court security may be prohibitive for reasons of cost or organizational resistance, several nationally known security assessment teams have developed a series of steps in phases that courts may take to achieve best practices. (See Appendix B.)

An example is weapons screening. A recommended best practice is universal entry screening. Everyone coming into a courthouse should be screened: judges, court staff, attorneys — everyone. Another best practice is to have at least one screening station consisting of a magnetometer, x-ray machine, hand wand, CCTV camera, and duress alarm at every courthouse entrance, with three armed law enforcement officers using triple-retention holsters operating each station.

These recommended best practice guidelines may not be readily achievable because of cost and acceptability. In that case, the recommended first phase consists of a series of steps that may involve relatively little cost or controversy, including the designation of only one door through which the public can enter the courthouse and, if necessary, another door permitting judges and staff to enter at a separate, private entrance; the assignment of one law enforcement or security officer to guard the public entrance; a table or other physical structure at the public entrance to serve as a screening station; a screening process for the public coming into the courthouse, which includes the use of a hand wand and the physical search of personal items (*e.g.*, purses and briefcases). From these first steps, there are other phases that a court may go through before reaching the final phase of best practice, with its vision of screening everyone at a station that contains a magnetometer, x-ray machine, duress alarm, and CCTV camera.

Planning and Budgeting

Once the results of the self-audit have been evaluated, members of the Security Committee, in concert with law enforcement officials, will need to decide what corrective steps must be taken to cure deficiencies in security and in what order of priority. The Security Committee should first rank-order the vulnerabilities and risks. Then, working through designated task forces or subcommittees, if it so chooses, the Security Committee should consider the most cost-effective means for mitigating the risks and implementing changes. Mitigation of risks and implementation of change can be strategically spread over a multi-year

scenario to provide time for seeking and allocating sufficient funds to get the job done. As noted previously, some items can be addressed at little or no cost. These include primarily intangible items such as promulgating policies and procedures, improving communications, and sponsoring security training. Other items may be more costly, like establishing and operating one or more weapons-screening stations or purchasing and installing electronic access and alarmed emergency exit systems on doors.

Ongoing Management of Courthouse Security

Finally, once plans have been established and budgets acquired, the court, through its Security Committee, must remain constantly vigilant in overseeing the implementation of security plans and improvements. Quarterly progress reports should be thoroughly analyzed by Security Committee members to make sure the most significant risks are being appropriately addressed, mitigated, and eliminated. Follow-up court security audits should be undertaken periodically in order to assess progress. Security self-audits should be repeated no less than every other year. Spot audits with respect to the areas of greatest risk should be taken more frequently. Information gathered and analyzed as part of a solid incident reporting system can also provide an additional basis for audits. (See Chapter 6 on Essential Element 6 – “Incident Reporting.”)

It is important to note that self-audits are not limited to the courthouse. Judges and court staff can benefit greatly from conducting safety and security audits of their homes. They can also perform assessments of their own personal safety to and from work and in other non-work contexts. Resources to enable judges and court staff to engage in these efforts are set forth below in “References/Resources.” (See Appendix C.)

Postscript

Operating a program of effective courthouse security is not a one-time achievement. It is a serious and continuous goal for a court and requires constant monitoring. Improving court security must be a priority every day for all those interested and involved in the process. The risks involved in courthouse operations are great and varied and may never be totally eliminated. With proper attention, care, and support from court leadership and law enforcement officials, risks to personal safety and security can be minimized. Successfully conducting security self-

audits and implementing remedial plans resulting from such audits can significantly assist courts in minimizing risks and, thereby, securing access to justice.

References/ Resources

National Sheriffs' Association
1450 Duke St.
Alexandria, VA 22314
(800) 424-7827 / (703) 836-7827
Fax (703) 683-6541
<http://www.sheriffs.org/>

U.S. Marshals Service
Addresses and phone numbers for district offices listed on Web site.
<http://www.usmarshals.gov/>

International Association of Chiefs of Police
515 N. Washington St.
Alexandria, VA 22314
(800) THE-IACP
Fax (703) 836-4543
www.theiacp.org

The National Judicial College
Judicial College Building/MS 358
Reno, Nevada 89557
(800) 25-JUDGE
www.judges.org

National Center for State Courts
300 Newport Ave.
Williamsburg, VA 23185-4147
(800) 616 -6164
Fax (757) 220 -0449
www.ncsc.org

The Justice Management Institute
1888 Sherman St., Ste. 410
Denver, CO 80203
(303) 831-7564
Fax (303) 831-4564
www.jmijustice.org

Policy Studies Inc.
1899 Wynkoop St., Ste. 300
Denver, CO 80202
(303) 863-0900 / (800)-217-5004
Fax (303)295-0244
<https://www.policy-studies.com>

ASIS International
1625 Prince Street
Alexandria, Virginia 22314
(703) 519-6200
Fax (703) 519-6299
www.asisonline.org

Note: There are many court security experts (directors and their security staffs) who presently work for state court administrators in administrative offices of state courts who are able to provide technical assistance for a self-audit of a court building.

Publications

Bell, Chief Judge R. M. “Improving the Security of Our State Courts.” Arlington, VA: Government Relations Office, National Center for State Courts. May 3, 2007.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=110>.

Casey, P. “A National Strategic Plan for Judicial Branch Security.” Williamsburg, VA: National Center for State Courts. 2006.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=80>.

Fautsko, Timothy F. “Post 9/11: Are Courts Really Secure?” *Annual Report on Trends in the State Courts*. National Center for State Courts. 2001.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=129>.

Fautsko, Timothy F. “Entry Screening – The Court’s First Line of Defense.” *Annual Report on Trends in the State Courts*. Williamsburg, VA: National Center for State Courts. 2008.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=117>.

Fautsko, Timothy F. “Taking Precautions: 101 Personal Safety Tips for Judges and Court Staff.” Denver, CO: National Center for State Courts. 2009.
http://contentdm.ncsconline.org/cdm4/item_viewer.php?CISOROOT=/facilities&CISOPTR=143&REC=1.

Franklin, Malcolm. "Ensuring the Personal Security of Judges." *Future Trends in State Courts 2009*. Williamsburg, VA: National Center for State Courts. 2009.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=147>.

Raftery, W. E., ed. "Mini-Symposium on Court Security." *Justice System Journal*. Vol. 28, No.16. 2007. <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=96>.

National Sheriffs' Association (n.d.). "Physical Security Checklist, Form 1.2.1." *Trial Court Performance Standards and Measurement System*. Williamsburg, VA: National Center for State Courts. www.ncsconline.org/D_Research/tcps/Forms/Form_1_21.pdf.

National Sheriffs' Association and Court Officers' and Deputies' Association, "Court Security Resource Guide: A Practical Guide to the Practices, Procedures and Resources Available for Those Providing Court Security." 2008.

National Association for Court Management Court Security Subcommittee. "Court Security Guide." Williamsburg, VA: National Association for Court Management. 2005.

Chapter 3: Emergency Preparedness and Response: Continuity of Operations (COOP)

Court operations are by their very nature both essential and vulnerable. They are essential as a necessary and vital ingredient to preserving the rule of law that is a cornerstone for our way of life in this country. They are vulnerable because they take place in buildings susceptible to disruption caused by a variety of manmade as well as natural emergencies or disasters. The list is long and can be frightening. In terms of natural hazards, there is the possibility of storms, lightening, floods, hurricanes, earthquakes, fires, and pandemic illnesses such as H1N1 Swine Flu. Human-caused emergencies include vandalism, arson, hostage-taking, prisoner escape, and attacks by aggrieved litigants. Under the banner of terrorism, there is a host of potential hazards that include nuclear, biological, and chemical agents.

Manmade emergencies or disasters such as bombings are, to a degree, preventable through the implementation of best practices in courthouse security. Natural emergencies, or disasters such as floods or earthquakes, may strike and disrupt court operations without any effective means to prevent them.

In this century, one of the most striking natural disasters affecting court operations was Hurricane Katrina in 2005. According to newspaper accounts, some examples of the sorts of havoc wreaked in a court system that ceased to function in the wake of this enormous natural disaster included the following:

- The courts struggled to account for and properly process more than 8,000 New Orleans area inmates evacuated to 34 jails around the state. The result was an influx of *habeas corpus* petitions from prisoners held for unlawfully long periods of time due to the absence of judicial forums to screen cases and set conditions of release, the unavailability of essential justice system personnel and court records, and the collapse of funding for the public defender system. In some cases, there was little choice but simply to release dozens of inmates without bail after weeks or months of imprisonment, potentially creating a hazard to public order and safety.
- The justice system also faced significant public safety challenges in accounting for defendants out on bail, convicted offenders on parole or probation, and registered sex offenders.
- As soon as the New Orleans courts relocated to temporary sites around the state, there was an increase in child custody and support cases. When they reopened in New Orleans, there was a surge of domestic violence petitions, divorce filings,

- and custody/visitation proceedings occasioned by the relocation of custodial parents.
- The courts were quickly deluged with eviction proceedings as landlords sought to take possession of properties in an effort to begin repairing and releasing them to new tenants.
 - The courts were inundated with storm-related lawsuits involving insurance coverage, victim compensation, property damage, and commercial losses.
 - Until the court system was remobilized, obligors had no clear route for making child-support payments.

The public in our communities expect courts to continue to function during an emergency and to resume full operation in a timely fashion after the emergency has passed. Court management has a responsibility to have comprehensive emergency preparedness plans in place, to test those plans, and to effectively communicate the protocols and procedures contained in the plans to all those who have a need to know. Local court management may look to the state or elsewhere for consultation, but in the final analysis, the citizens of each community expect their local court officials to have appropriate emergency plans in place.

Clearly the time for thinking about what to do in the case of an emergency or disaster is long before the emergency or disaster strikes. Planning is the key to success, and there are commonly three kinds of plans.

1. **Emergency preparedness plan** – covers what to do in the case of a variety of specific emergencies (*e.g.*, fire, bomb threat).
2. **Continuity of operations (COOP) plan**– encompasses how to withstand a serious disruption of court operations, to restore and continue essential business functions of the court.
3. **Disaster recovery plan** – focuses on how to retrieve and restore vital assets of the court, particularly records and information systems, in the aftermath of a disaster.

This chapter covers the first two kinds of plans. Chapter 4 will discuss disaster recovery.

Plans are essential tools in emergency management. NCSC has developed a strategic framework for emergency management that will allow court management to take a logical, structured, and comprehensive approach to dealing with these serious matters. The framework encompasses six factors:

1. Management
2. Prevention
3. Preparedness
4. Response
5. Recovery
6. Training

Management

The first factor to consider is management. Leadership is the foundation for effective emergency planning in state courts. Each chief justice (CJ) and state court administrator (SCA) needs to set the tone for the entire judicial branch by demonstrating a leadership commitment and by sending the message that emergency planning and preparedness is a top priority that must be integrated into the state's judicial culture. In addition to policy statements and directives that emphasize this priority, a management mechanism needs to be put in place. Chief Justices should appoint a statewide committee to coordinate emergency preparedness efforts and recommend policies and guidelines for the entire judicial branch. The Chief Justice should designate a chief emergency preparedness officer to chair the committee and be the judicial branch's point person. Judicial districts and/or individual courts should likewise have their own standing committees dedicated to emergency preparedness issues.

It is also extremely important for courts to coordinate their emergency and disaster management efforts with those of other government agencies at the federal, state, and local levels. Good emergency planning requires an enormous amount of advance coordination among different court levels and between the courts and a host of federal, state, and local agencies on a wide range of facility, security, law enforcement, and emergency management issues. Unfortunately, many courts do not have a seat at the table when state and local emergency management agencies are at the planning stage. Nor have the state courts been very proactive in reaching out to these agencies to help them understand how important it is to keep the courts open to address the immediate justice needs of those experiencing disaster-related upheaval. Regular outreach and communication with emergency management officials in the jurisdiction will help ensure that every court is perceived and treated as a priority and integrated into state and local emergency management networks and planning processes.

At the federal level, the Federal Emergency Management Agency (FEMA) is critically important to disaster management because it coordinates all assistance provided directly by the federal government to declared emergencies and provides federal grants to cover many emergency costs, including repair, restoration, and reconstruction of public facilities. Courts need to develop a strong understanding of FEMA's workings and of the basic legal framework governing federal disaster preparedness and recovery.

Courts should consider how best to organize a team to develop a COOP plan. To begin drafting (or adapting) a COOP plan on the state level, consider recruiting district court administrators from large, medium, and small counties. These valuable employees have the experience to think through any plan or proposal, and their contributions will be invaluable. An attorney from a court rules committee could be helpful, since he or she will be able to identify legal issues and concerns. On a local level, the organizational team structure for drafting and implementing the COOP plan will vary depending on the size and complexity of each court system. A one-size-fits-all approach might not work because of the unique character of each jurisdiction. A key factor in determining the structure is the number of personnel available to conduct the numerous functions associated with COOP implementation.

The COOP team must be large enough to represent the core areas the plan will cover but small enough to work efficiently. The size of the committee will necessarily vary from jurisdiction to jurisdiction. It is probably best to err on the side of making the committee too small when the process begins because it can always be enlarged if necessary to add representatives from additional areas.

Some stakeholders should be involved on a limited basis. These contributors need not be full members of the committee but should only be consulted for input in particular areas of their expertise. They would not be involved with forming the overall plan. Some stakeholders — both internal and external — may have a more specialized role in assuring continuity of operations, and they can be asked to participate as needed.

Prevention

The second factor to consider in emergency management is prevention. Prevention efforts are designed to protect occupants and visitors in court facilities as well as the facility itself and the property inside the facility. Steps for prevention in the area of court safety and security are discussed in other chapters of this handbook (Element 1, “Operating Procedures;” Element 2, “The Self-Audit of Court Facilities;” Element 5, “Threat Assessment;” Element 6, “Incident Funding;” and Element 10, “New Courthouse Design”). The key to prevention is performing regular and systematic assessments to identify areas of risk within and around the court facility and then instituting a rational, comprehensive process for mitigating those risks.

Preparedness

The third factor to consider in emergency management is preparedness. It is here that planning becomes crucial. As indicated above, three kinds of plans may be appropriate: emergency preparedness, continuity of operations (COOP), and disaster recovery. Plans can be developed separately or can be made part of one overall plan.

Plans to prepare for and respond to emergencies should include at least the following components:

- **Evacuation protocols** to get people to safety, notify emergency responders, and salvage vital records and physical assets.
- A clear **provision for “who is in charge.”** In a crisis, command and control are essential.
- **Communication protocols** to keep key staff apprised of the status of the emergency and whether, when, and how to report. A key element is a “phone tree” that lists who needs to be contacted first and who is responsible for contacting whom. The phone tree should include home and cellular phone numbers, pagers, and other contact information. Court leaders and key staff, including security personnel, should all be provided with the current phone tree lists ahead of time. Along with phone trees, emergency preparedness Web sites and telephone hotlines can serve as additional means for providing staff with necessary information.
- A **system for identifying employee location and status** in the aftermath of an incident.
- A **designated assembly site** so that building occupants know where to go during an evacuation.

Continuity of operations (COOP) plans ensures courts know what to do if faced with an emergency that threatens continuation of normal operations. Traditionally, a COOP plan is developed and implemented for situations in which the courthouse or court-related facilities are threatened or inaccessible (*e.g.*, as a result of a natural or manmade disaster). A traditional COOP plan establishes effective processes and procedures to deploy quickly pre-designated personnel, equipment, vital records, and supporting hardware and software to an alternative site in order to sustain organizational operations for up to 30 days. It also covers resumption of normal operations after the emergency has ended.

A COOP plan for courts should include the following:

- Specific objectives for the COOP plan relating to the court’s mission and functions
- An overall approach for maintaining essential functions during an emergency
- Emergency roles and responsibilities of organizations and positions
- Orders of succession to key positions and arrangements for pre-delegation of authority for making policy determinations and decisions
- Essential court functions and staffing, plus the resource requirements for each
- Measures to protect all vital records, databases, and information systems needed to support the court’s essential functions
- Alternate operating facilities capable of immediately supporting the performance of essential functions under various threat conditions
- Preparations for emergency relocation of COOP contingency staffs to alternate facilities
- Interoperable communications requirements for the alternate facility to ensure the availability and redundancy of critical communications systems
- A basis for training COOP participants, testing equipment, and conducting exercises to evaluate specific aspects of COOP plans, policies, procedures, systems, and facilities
- A multi-year strategy and program management plan for developing and maintaining COOP capabilities

A court COOP plan should also include provisions for the resources of other agencies that may be required in the performance of the court’s essential functions and consideration of how the continued performance of the court’s essential functions will affect or, in turn, be affected by other state, county, and local offices.

More recent COOP planning also takes into consideration the impact a pandemic could have on normal court operations. Although the court facility might remain intact, normal operations could be suspended, likely for 90 days or more, because — due to quarantines, sickness, or death — there would be too few individuals to perform the court’s work or work on which the court relies (*e.g.*, jury duty, prisoner transporting, mail delivery, sanitation activities, equipment repairs). Under these conditions, pandemic-specific aspects of the COOP plan may be activated even though the court facility is not damaged.

The National Center for State Courts (NCSC) has developed an extensive COOP planning guide and template, which are available online at the NCSC Web site. The guide and template were prepared by NCSC with the assistance of a national coalition of leaders from all sectors involved in business continuity planning for courts and was supported by the U.S. Bureau of Justice Assistance (BJA). The template provides a step-by-step approach to help courts develop and maintain a viable COOP capability.

Disaster recovery plans, which focus on the retrieval of vital records and information systems, are the topic of the next chapter of this handbook.

Response

The fourth factor to consider in emergency management is response. At this point, an emergency or disaster has occurred. Now is the time to activate and implement the plans, including relocation of essential functions to alternate sites.

Recovery

The fifth factor is recovery. This includes steps to return court staff, operations, and infrastructure to the condition in which they were prior to the time that the emergency or disaster occurred. This also includes the recovery of information technology (IT) systems and data. These topics will be covered in Chapter 4 of this handbook.

Training

The sixth and final factor to consider is training. Although this factor is presented last, it in fact encompasses all of the prior factors, which will prove of little value unless judges, court staff, and emergency response teams are fully trained in how they should respond in a crisis. Training and testing of emergency plans are imperative. By testing and practicing plans (*e.g.*, tabletop exercises), court emergency managers can identify gaps and strengthen plans. Further, simulated exercises help the emergency responders rehearse so that if and when a real emergency or disaster occurs, they will be better prepared to discharge their duties.

Emergency Preparedness in Dependency Courts

In addition to the six factors discussed above, special consideration must be given to emergency preparedness in dependency courts. When a court assumes jurisdiction over a child, the court also assumes the responsibility that a parent would have to protect the child's best interests and welfare. This responsibility becomes particularly keen in the event of an emergency.¹

Professionals serving children and families are familiar with the perspective of trying to view problems "through the eyes of a child." This perspective is even more important in times of crisis. The "needs of the children" should be kept foremost in all emergency preparedness planning. The Adoption and Safe Families Act of 1997 (PL 105-89) clearly and unequivocally establishes three national goals for children in foster care: safety, permanency, and well-being. These goals assume even more significance in times of emergency. Safety of children is in more jeopardy during times of crisis where they may not be in the homes of parents, relatives, or foster parents, but in transit, in temporary shelters or even on the streets or in other locations where they may be in danger.

Of the 5000 children who were in foster care in Louisiana at the time of Hurricanes Rita and Katrina, nearly 2000 were displaced. Federally mandated judicial

¹ This section incorporates information from prior collaborative efforts of the ABA, NCSC, NCJFCJ funded by the Children's Bureau of DHHS. The entire document is on line at <http://www.icmeducation.org/katrina/Introduction.html>.

oversight of those 2000 displaced children was disrupted and delayed, thus threatening their safety, permanency and well-being. Immediately after the hurricanes and even a year later, many children under court jurisdiction were no longer living within the geographical jurisdiction of their court of origin.

No one anticipated the extent of the devastation caused by Hurricanes Katrina and Rita, and many were unsure of what was expected of them in a crisis of this magnitude. The safeguards that Louisiana and Mississippi built into their laws, policies, and procedures did not anticipate the extent of the devastation and could not adequately protect their children from the effects of the hurricanes.

In promoting the safety of children, courts should carefully address the following concerns.

Emergency Preparedness and Planning

- Creating a specialized emergency preparedness plan for dependency courts.
- Integrating the dependency court emergency plan within the court's over-all plan.
- Coordinating and sharing the court's emergency plans with stakeholders.

Without dependency-specific disaster planning, courts, child welfare and juvenile justice professionals, and advocates cannot share information or coordinate essential activities. Courts and agencies cannot locate children and foster and biological families, provide critical services and supports, and ensure appropriate oversight of cases. Courts cannot make best interest determinations, enforce or modify custody orders, or transfer jurisdiction as needed. In short, without emergency preparation and planning, courts cannot discharge their responsibility for serving the best interests of the child.

An emergency preparedness program applies to any threat or emergency that may disrupt normal court operations. It should be multidisciplinary and incorporate all facets of court operations, including case management, administration, technology, security, human resources, and facilities management. Stakeholders should embrace the concept of shared responsibility for the program and related training activities.

For dependency courts,² a viable emergency preparedness program requires coordinated efforts within the dependency court itself, with other sections of court and courts in the same jurisdiction (including appellate courts), with dependency courts in other areas of the state or region, and with critical stakeholders including social services departments, local law enforcement, and emergency responders to prevent, prepare for, respond to, and recover from a broad array of disruptions.

Dependency courts should be involved in plans related to prevention, preparedness, response, and recovery, including continuity of operations plans, occupant emergency plans, evacuation and critical incident plans, shelter-in-place plans, disaster recovery plans, emergency procedures, and security.³ Scarce resources should not prevent planning for emergencies.

An important planning resource for dependency courts is the National Association for Court Management's Business Continuity Management Mini Guide (2006), the appendix of which contains examples of a business impact analysis questionnaire, a mission essential-function template, FEMA's COOP planning guidance, and orders of succession, as well as a delegation-of-authority worksheet and a continuity-of-operations planning checklist. Although not dependency court specific, a template for assessing the status of COOP planning has been developed by the Bureau of Justice Assistance at the request of the Louisiana Supreme Court.⁴

For dependency courts, it is especially important to carefully plan evacuation so that the judge, court clerk, and others necessary to hold hearings would all be evacuated to the same location and so that parties, attorneys and other stakeholders would know where hearings will be held. In addition, court personnel should have agreed-upon places to report to if the emergency extends beyond the immediate area. Once relocated, judges

²This document uses the term "dependency court" to refer to courts hearing cases involving abuse, neglect or abandonment of children and youth. However, the provisions of this document and the responsibility of the court would also extend to youth removed from the custody of a parent and otherwise placed in state custody pursuant to state and federal law (specifically Title IV-E, Foster Care).

³ For example, *see* Jefferson Parish, (Louisiana) COOP, available at: www.jpjc.org/WebContent/Downloads/COOP.doc.

⁴ Template for Assessing Status of COOP Planning: Louisiana District Courts. BJA Criminal Courts Technical Assistance Project, American University. TA Assignment Number 4-134 (May 2010).

can adjust their individual calendars to accommodate the transfer of emergency matters from other calendars.

The dependency court needs to identify which of the courthouse's plans specifically include them and which parts of the above detailed plans should be created specifically for the dependency court. The Mission Essential Functions Template (http://www.flcourts.org/gen_public/emergency/bin/Mission%20Essential%20Functions%20Template.doc) from the Florida State Courts Emergency Preparedness web site might be helpful in prioritizing court functions in the event of an emergency.

Communication

Specifically, identify and incorporate dependency court needs in the court's COOP:

- Ensure the ability to communicate with others in an emergency.
- Establish alternate modes of communication.
- Identify emergency spokesperson(s).
- Inform the public.

Communication is vital to response and recovery of court operations both during and after an emergency. In the event of an emergency that suspends court operations for even part of a day, the dependency court must be prepared to establish or restore communication among court leaders, between its judicial officers and personnel, and with external stakeholders, such as child welfare agencies, families, dependents, and attorneys.⁵

It is important to know how the dependency court fits into the entire courthouse's critical incident, evacuation, disaster recovery (IT), and continuity of operations plan (COOP). The dependency court is likely to be tied into the courthouse's plan for recovering or repairing the general communications infrastructure. However, the dependency court should take its own measures to ensure that key personnel have the necessary contact information for court personnel, attorneys, guardians ad litem, court-

⁵ The New Jersey Judiciary's COOP planning includes an alternate location for hearings, communication with the public and single sources of communication.

appointed special advocates (CASAs), foster parents, and social services agencies, and that they in turn know how to contact the court.

While it is probably not possible for the dependency court to prepare for each and every communication contingency, at a minimum the dependency court must be ready to initiate some alternative modes of communication (*e.g.*, alternate land lines, satellite phones, Nextel-type radios, text messaging, media announcement template). Key personnel need to know how to contact all court personnel and dependency court stakeholders such as attorneys, foster families, and social services agencies. Having one of these elements without the other will delay the court's ability to perform essential functions and resume normal operations.

Federal judicial branch COOP plan developers recommend the following actions to support communications in times of emergency: have alternate e-mail addresses for judges and court staff; maximize the use of available media, including e-mail, radio, TV, and external Web sites, for both internal communications and communications to the public; and have satellite phones charged and staff who know how to use them.

Emergency notification may be communicated through a variety of media, including: a court emergency telephone notification system; public announcement system; court web sites; electronic mail (e-mail); recorded telephone messages; announcements on local radio and television stations; and in-person communication. Multiple technologies should be employed when possible because communications failures are inevitable in an emergency.

Emergency planning should include development of a centralized "go to" contact for dependency court stakeholders. Such a website or phone number known in advance can provide ready access to needed information, including the status of the emergency plan implementation.

The court should designate one person and one alternate with authority to speak for the court to ensure accurate and consistent information is imparted. This person could be the same as the spokesperson for the entire court. If the media are not including information about court operations in their briefings, other government agencies may be willing to include the courts in their briefings. The dependency court can also print announcements in local newspapers, use the court's Web site, maintain an information

hotline at the court, or provide a toll-free number for the public to call for court information.

Identifying and Locating Children, Families and other Parties

The court should implement several policies and procedures to assist in identifying and locating children and families. Courts should consider:

- Using CASA volunteers to locate children.
- Having shelters automate lists of residents to facilitate locating children, contacting their legal custodian, and reuniting children with families or foster families.
- Advocating for child care and protective order/offender screenings at all emergency assistance centers.
- Encouraging visitation of children displaced to other locations.
- Making agreements on health coverage part of interstate compacts. Facilitating continuation of federal and state benefits and services to children during displacement.

As Hurricanes Katrina and Rita demonstrated, if a disaster disrupts court operations, ready plans are critical to protect children under the court's jurisdiction. The emergency steps described above will be possible only if there has been strong advance preparation and quick organizational adjustments following the disaster. Establishing plans that take into account the expeditious location of children, and ensuring that key court personnel and participants in the court process are aware of the specifics of the plan will go far in reducing confusion and emotional impacts.⁶

⁶ In New Jersey the Division of Child Protection and Permanency and the judiciary have access to each other's database thereby allowing them to access case information on each child. However, the judiciary does not have responsibility for any shelter or the location of children.

The document *Ensuring the Unique Needs of Dependency Courts are Met in Disaster Planning Efforts: Dependency Court Planning Templates for Continuity of Operations Plans* provides helpful templates for establishing a Continuity of Operations Plan to meet the needs of children placed in state care.⁷

Jurisdiction

- Examine relevant law (constitutions, statutes, court rules) regarding jurisdictional authority.
- Establish jurisdictional flexibility and continuity through statutes or court rules for judicial emergencies.
- Pre-determine how the court will operate in an emergency, including the status of scheduled hearings and current court orders.

It is important to consult the relevant state constitutional and statutory provisions that confer jurisdiction on the trial courts that adjudicate dependency cases. Also, state court procedural rules should be reviewed to ensure local courts have the authority and flexibility to function during and after an emergency.

Those in vulnerable situations look to consistency to provide stability. Appearing before the same judicial officer in the same courthouse is a child-welfare best practice that provides that sort of consistency, even if the events and life of the dependent are changing from foster care to family, from family to temporary protective placement, or any one of the myriad of changes that can occur in the course of abuse and neglect cases. However, events as simple as a water-main break and as complex as a major natural disaster can change this, forcing the foster child to (at best) go to a different courthouse

⁷ *Ensuring the Unique Needs of Dependency Courts are Met in Disaster Planning Efforts: Dependency Court Planning Templates for Continuity of Operations Plans*, National Council of Juvenile and Family Court Judges and American Bar Association, Center on Children and the Law (2008), available at: <http://www.ncjfcj.org/resource-library/publications/ensuring-unique-needs-dependency-courts-are-met-disaster-planning> (accessed June 2012). Designed to improve data-sharing practices and thereby improve outcomes for youth involved in the juvenile justice system, the *Models for Change Information-Sharing Toolkit* includes supporting documents such as consent forms, templates, memoranda of understanding, and recorded webinars (Models for Change, 2008). Available at: <http://www.modelsforchange.net/publications/282> (accessed June 2012).

See also: *National Commission on Children and Disasters. 2010 Report to the President and Congress*. AHRQ Publication No. 10-M037, October 2010. Agency for Healthcare Research and Quality, Rockville, MD. <http://www.ahrq.gov/prep/nccdreport/> (accessed June 2012) for a full report which includes templates and other materials.

or a different judge or (at worst) flee the area and take residence elsewhere in the state or even the country. Reestablishing normalcy in process, services and relationships by returning to pre-emergency conduct becomes essential for the safety, permanency, and well-being of foster children.

Courts must balance the need for consistency in terms of places where hearings are heard and the need to address ongoing emergencies as they occur. Courts must have this authority and flexibility established long before the emergencies occur. In the case of Hurricane Katrina, the federal district courts simply moved first and then sought legislative approval of the relocation outside their assigned districts. The state courts in many cases were not so fortunate because the state legislatures were unable to convene. The trial courts were forced to rely on their inherent powers and issue orders themselves or await orders as directed by their state courts of last resort.

For legal authority to address emergencies and changing conditions, the court may be able to rely on the power granted by the constitution or statutes in terms of planning for an emergency, functioning during the emergency and executing a recovery effort after the event. It is important to consult the relevant state constitutional and statutory provisions that confer jurisdiction on the trial courts that adjudicate dependency cases to ensure court leaders know the scope of their authority to act. The lack of explicit constitutional or statutory provisions arguably means that the court must rely exclusively on its inherent powers or on the powers of the judicial branch in general to perform its governmental obligation.

Some states, such as California and Georgia⁸ have enacted statutes that authorize courts to take extraordinary measures in the aftermath of a disaster. Other states, such as Pennsylvania⁹ have authorized similar measures through Supreme Court rule. New Jersey

⁸ California Code, Section 68115-68118; Official Code of Georgia Annotated, Sections 38-3-60 to 38-3-64. The California statute authorizes the holding of sessions anywhere within the county or transferring civil cases to an adjacent county in an emergency, “notwithstanding any other provision of law.” The Georgia statute enables an authorized judicial officer to “declare a judicial emergency and designate an alternate facility in lieu of court.”

⁹ 42 Pennsylvania Consolidated Statutes Annotated, Section 931; Pennsylvania Rules of Judicial Administration, Rule 1950-1954. The Pennsylvania statute extends the county trial courts process “beyond the territorial limits of the judicial district.” The Pennsylvania Supreme Court rules provide for the declaration of a judicial emergency to permit the suspension or modification of court rules by “emergency judicial order” and designate counties to act as “emergency regional administrative units.”

also has provisions for the judiciary to maintain jurisdiction of cases in any county in the state and to conduct hearings by alternative methods. In all of these, emergency planners have vested considerable authority in local court leaders to take a myriad of actions that may be necessary to keep courts functioning. Relevant to the question of jurisdiction is how such jurisdiction will be exercised. For example, can the court operate outside its territorial jurisdiction? Can the court hear cases on an emergency basis as a courtesy to other courts? Do the parties need to be physically present in court for the matter to be heard or can the court operate via video or telephone? How will orders and other information be recorded? Where will documents be filed? How will service be made? How will notice be provided?

Confidentiality

- Assess informational needs and confidentiality barriers.
- Collaborate with IT and stakeholders.
- Facilitate access to confidential case record information through
 - statutes and court rules
 - emergency credentialing
 - integrated juvenile justice system, especially to facilitate recovery and back-up
 - cooperative agreements
 - orders of succession / delegation of authority

Dependency courts must continue to operate in spite of disaster conditions, including damage to their physical facilities. Dependency courts may need to proceed without all stakeholders present. Stakeholders may be absent after a disaster due to a change in geographical location for hearings, loss of communications, incapacitation, evacuation, or other reason. However, the absent stakeholders may still be keepers of records that are needed for hearings to proceed or to ensure quality decisions.

One of the important components of any disaster preparedness plan is to facilitate access to records by stakeholders who legitimately need access. Without prompt and appropriate access to paper and electronic records, stakeholders cannot perform their duties in a timely and quality fashion.

A disaster creates three categories of child protective system stakeholders: stakeholders that are on-site and attempting to carry out their responsibilities under trying conditions; absent stakeholders who are not available to carry out their everyday duties; and new stakeholders whose presence in the child protective system is dictated by the disaster conditions. A disaster can raise cross-jurisdictional issues with record confidentiality that would not arise under normal conditions.

The child protection system today is a large and interconnected web bringing together stakeholders from the judicial branch, the executive branch, and the public and private sectors. Each stakeholder maintains its own set of records, often in both paper and electronic form. Dependency records, whether from the judicial or executive branch, are predominantly confidential in nature, and confidential clearance is required to view the records. Access can be established through various legal authorities, such as statute, court rule, or a court order. Often, the deciding factor in granting access by court order is whether the requestor has a “legitimate interest” or “direct interest” in the case. The large number of stakeholders from disparate fields with different institutional world views, coupled with the confidentiality of the records, contributes to the complexity of dependency matters, and sometimes contributes to delays in process and decision making.

Confidential records in the child protection system raise unique problems in emergency planning. Recovery staff not only must facilitate access to paper and electronic records in a timely manner, but also must do so lawfully—in accordance with confidentiality requirements. Recovery staff cannot ignore confidentiality requirements or take “short cuts” to provide quick access to stakeholders. They must follow existing law, policy, and procedure—unless special disaster-recovery provisions or contingencies are in place that either deliver immediate access or relax requirements in disasters to deliver access to those who legitimately seek it.

Information shared between the stakeholders includes information that would be considered confidential, including treatment plans, programs and services the juvenile participated in, worker history, current medications, and substance abuse. However, each agency can decide to restrict its information to a smaller subset to safeguard confidentiality.

Confidentiality rules serve an important function, i.e., to protect the privacy interests of children and various stakeholders, but other interests may outweigh these privacy interests in the wake of disaster. For example, in times of disaster, protection of a child from abuse and neglect is in the best interests of the child and might outweigh protections of confidentiality. This is not to suggest that we should abandon our regard for confidentiality rules across the board, but we need to recognize that certain exceptions may exist in times of exigency, when both victim protection and confidentiality cannot be simultaneously accomplished. In response to Hurricane Katrina, HIPPA confidentiality requirements were relaxed so that health care providers were authorized to speak with family members, even if a patient was unable to grant permission to do so.¹⁰ Dependency courts must act on critical pending matters, even if all regular stakeholders are not available, and confidential records should not be a reason for delay. Stakeholder substitutions and delegation of authority must be allowed in certain circumstances.

Dependency courts should: examine existing record recovery plans and consider the needs of stakeholders to have access to confidential records in the child support system after a disaster; instruct information technology professionals, records management professionals, and other disaster recovery planners of special issues in dependency matters and the need for a separate, comprehensive plan to ensure the continuation of timely and quality decisions; and work with other institutional stakeholders in the state to ensure that they take the same course and participate in cooperative record-access planning across the state child support system in preparation for disaster.

Access to confidential information can be addressed in the following ways:

Statutes and Court Rules

Statutes and court rules can be promulgated to facilitate the sharing of information between agencies and between governmental branches. Child protective stakeholders should work with legislative committees and the courts to define the emergency circumstances that warrant a conditional exception to confidentiality restrictions.

¹⁰ See APHSA policy memo available at www.aphsa.org/katrina/docs/Policy-Memo-9-30-05.pdf.

Juvenile confidentiality statutes and court rules could contain a “Disaster” or “Emergency” provision, such as: “Confidentiality requirements may be temporarily waived when they hinder other more important goals of the dependency court, such as identification or protection of a child.” For example, Minnesota has facilitated access to confidential court records through court rule.¹¹ Colorado has minimized the obstacles to sharing information in delinquency, dependency and neglect cases through statute.¹²

Credentialing

Courts and other institutional stakeholders need to plan ahead and prepare a policy for emergency credentialing to provide outside stakeholders with emergency access to confidential information needed during an emergency. Disaster provisions could spell this out to the most detailed level of guidance possible, leaving fewer decisions to be made at the time of disaster.

Technology

Integrated juvenile justice systems which share juvenile information require a great deal of planning and work by the stakeholders to come into existence, but the reward is great under normal circumstances and even better in emergencies. Access to confidential information in the integrated systems can be controlled at many levels. An integrated juvenile justice system may allow retrieval of shared information when an entity’s files are destroyed, lost, or temporarily inaccessible.

Technology solutions can help mitigate the effects of a disaster. A complete electronic record, together with a comprehensive plan for backup and recovery, can make dependency records available under disaster conditions. First, stakeholders should keep complete electronic records which fully mirror paper records to allow for full electronic recovery of dependency case records. It is not enough for the electronic dependency record to consist merely of data in a case management system. Reports and other documents should also be captured and stored in electronic form—including the educational, psychological, diagnostic, and medical records. When disaster strikes and

¹¹ Minnesota Rule 8 of the Rules of Public Access to Records of the Judicial Branch.

¹² Colo. Rev. Stat. Ann. §19-1-303 (1998) (Appx).

access to records is compromised, the judge cannot afford to wait until the clerk can reconstruct this vital information from the original record custodians. Next, after building a complete electronic case record for all dependency matters, stakeholders should plan for 100% uptime for dependency applications and document access—also known as “24/7/365.” The plan should include replicated data, critical applications, and security policies at a remote “hot site.” This will ensure that the application is up and running, with current data and proper security, as soon as communications can be established from the disaster area or neighboring region. The stakeholder community should pool resources and work together with state government to develop hot sites to service them, when needed. If hot sites are not achievable, at a minimum all dependency records should be backed up to one or more remote geographical locations. Although remote data backups may not offer expedited access in a disaster, because applications have to be reloaded and data recovered from the backup media, they will at least preserve the record.

Cooperative Agreements

Cooperative and mutual aid agreements can be a vital resource during and after an emergency. Mutual aid agreements and assistance agreements are agreements between agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident. Agreements between agencies may facilitate, among other things, information and resource sharing, technical support and personnel assistance. When considered in advance of an emergency, cooperative and mutual aid agreements may resolve confidentiality and legal concerns, cost allocation and even liability considerations.

Dependency court administrators should consider what information and resources could be at risk during an emergency. For example, facilities could be compromised, court records could be inaccessible, and electronic data could be lost. Agencies within and outside the jurisdiction may have resources that would help the court rebuild or recreate records, and they may have facilities or equipment that would aid the court in resuming operations after a disaster. In addition to continuation of court operations,

agreements should be considered to provide continuity of services to children under the court's jurisdiction to the extent feasible.

Cooperative and mutual aid agreements executed by those with the authority to commit resources and assistance in an emergency can be an integral part of continuity of operations planning.¹³

Orders of Succession / Delegation of Authority

Orders of succession and delegation of authority are key elements in any court's COOP. For dependency court administrators however the court's general plans may not be sufficient, particularly with regard to confidentiality. For example, by law, court rule or mutual aid agreement, certain individuals may be designated as points of contact or decisions makers. If those individuals are unavailable in an emergency, the dependency court's ability to obtain or share otherwise confidential information may be compromised. Ensuring that legal authorities (i.e. statutes and court rules) allow for the delegation of authority, and that cooperative or mutual aid agreements specify who is "next in command" when key decision makers are unavailable is critical. As with the court's general COOP, specifying several successors for key decision makers charged with protecting, receiving or sharing confidential information is crucial.

Protection of Court Records: Storage and Recovery

The protection and availability of vital records, databases, and information systems needed to support essential functions is a vital component of preparedness and planning. By taking the proper steps, courts can minimize the impact of disasters and thereby avoid the loss of records and the need to undergo recovery and salvage efforts. The less damage caused to records by disasters, the less disruption will occur and the easier it will be to resume operations. Plans for storage of dependency records should prioritize ready accessibility due to the time sensitive nature of these cases. In addition,

¹³ See www.mmrs.fema.gov/emergency/nims/ResourceMngmnt.shtm for more information about mutual aid agreements as well as this document, outlining best practices and lesson learned: <http://www.homelandplanning.nebraska.edu/Documents/radioconference/moreusefulmaterials/Best%20Practice-Mutual%20Aid%20Agreements-Developing%20Agreements.pdf>.

dependency records should be stored in a manner that is designed to maintain their confidentiality in the case of a disaster and recovery. Courts should consider the following steps:

- Conduct a building inspection to familiarize personnel with potential risks to records. Make any practical repairs or changes to mitigate the risks.
- Do not store records under plumbing or in areas that leak.
- Store records off the floor on sturdy shelves.
- Store records on an upper floor if the court's facility is located in a flood-prone area.
- Maintain constant temperatures below 65°F in dedicated storage areas, or 70°F in work areas occupied by personnel. Maintain relative humidity levels of 40 to 50%.
- Install fans and commercial dehumidifiers if high humidity is a constant problem and cannot be controlled with an adequate HVAC system.
- Store records out of direct sunlight and preferably in archival-quality containers.
- Consult a preservation professional about implementing a pest-control program.
- Create digital backups of all paper-based records. Store backups off-site and out of the geographical area.
- Establish and maintain a schedule to back up electronic data, usually daily or weekly. Store backups off-site and out of the geographical area.

Preparedness means having a response plan in place *before* a disaster. Besides identifying response, recovery, and salvage procedures and techniques to be used by a specific court in the event of disaster, a response plan should include other preparations that make recovery more efficient. These include the following:

- Take inventory of records—Note record format and media. Create a shelf-list.
- Prioritize records—Identify vital records and label records according to priority.
- Alternate site planning—Have an alternate site where the work of the court can continue and where recovered records can be housed.
- Develop and keep updated a recovery and salvage plan—Address options for the recovery and salvage of damaged records and make recommendations based on existing resources, personnel, and facilities.
- Establish a recovery team—Members should be authorized to view confidential records, trained in salvage and recovery, and well versed in the court's disaster response plan.
- Maintain an updated list of local emergency contacts.
- Maintain disaster response supplies.
- Maintain a list of response-and-recovery vendors and suppliers—Identify and establish contact with those vendors your court would be most likely to use in the event of disaster.

- Conduct an annual review—any disaster response plan should be reviewed every year.
- Cover storage areas with plastic sheeting to protect from water damage. (One of the biggest dangers to records in the event of a fire is damage caused by water used to extinguish the fire.)
- Move records to higher shelving to protect from rising floodwater.
- Move vital records off-site.

Hearings

Federal child welfare laws have been enacted to improve the quality and timeliness of dependency case decisions. A disaster, whether it is a simple loss of power or the total devastation of a courthouse or community, cannot be allowed to cause extensive delays in the proceedings of dependency courts that affect the safety, permanency, and well-being of children.

- Both state and federal law demand that courts proceed under specific and strict timelines and the occurrence of a disaster that disrupts court operations will not necessarily excuse states and courts from meeting such timelines.
- Aside from legal requirements, meeting the deadlines and avoiding long interruptions in child abuse and neglect cases is critical due to the child’s sense of time and need for permanency (Resource Guidelines, 1995; Flango, 2001).

The Adoption Assistance and Child Welfare Act of 1980, 42 U.S.C. §§ 620-629, 470-477, as amended by the Adoption and Safe Families Act (ASFA) necessitates more timely, decisive, and substantive hearings, and more frequent court and administrative case reviews. These include:

- Reviews at least once every six months
- Permanency hearings at least once every 12 months
- Petitions for the termination of parental rights by the time a child has been in foster care for 15 of the most recent 22 months

Other legal deadlines commonly found in state statutes or court rules include:

- Deadlines for hearings to determine whether to continue children’s emergency removal from home—state laws set deadlines mostly ranging from 24 hours to five days after removal.
- Deadlines for filing child abuse or neglect petitions—state laws set deadlines mostly ranging from the date of the emergency removal hearing to two weeks afterward.
- Deadlines for the completion of the hearing to decide whether the allegations of the petition are true (most typically called the “adjudication,” “fact finding,” or

- “trial”) to enable the court to assert its authority over the child. (Deadlines often range from ten days after removal to 90 days after removal.)
- Deadlines for the completion of the hearing to decide whether the state will be given custody of the child for placement into foster care—for children already removed from home, state laws impose deadlines ranging from 10 to 30 days after adjudication.
 - Deadlines for the completion of termination of parental rights proceedings (TPR)—state laws setting deadlines for TPR are frequently complex but often require the completion of TPR as early as within five weeks after the filing of the TPR motion or petition.

Whether or not a disaster has disrupted court operations, judicial timeliness is critical to achieving permanency. The harm to children from remaining too long in temporary care is compounded by the trauma of experiencing a disaster.

It may not be necessary for all participants to be physically present for all hearings. State law or procedure may permit connecting parties to the hearing by telephone or other audiovisual links. If parties and attorneys are scattered across state lines, this can be arranged pursuant to the Uniform Child Custody Jurisdiction and Enforcement Act (UCCJEA). How? Reports from other key stakeholders (e.g., service providers, foster parents) can be relayed by the caseworker or CASA, for example, to all parties at the hearing. It is also helpful to keep in mind that under ASFA a review hearing may be held sooner than six months and more frequently than every six months. Following an emergency, it may be helpful to set up a series of rapid review hearings, in person or by phone, with the parties to update everyone on the status of children and to make arrangements for displaced children or other family members.

The following are some key types of information that should be gathered before each hearing:

- The current location of the child and with whom the child is living.
- The current safety and protective arrangements for the child.
- Which parties and agencies have visited the child and currently have access to the child.
- The extent to which the child’s needs are being met, including services previously ordered, services currently provided for the child, services arranged, and when arranged services will be provided.
- Services previously ordered for the parents, services currently provided for the parents, services arranged, and when arranged services will be provided.

- How, when, and where will any visitation with the parent and sibling(s) commence.
- If applicable, how and when the child will return to school.
- If applicable, how and when the child will return to the child's prior placement.
- If applicable, how and when the child will return to the court's jurisdiction.

Training and Collaboration

Training activities are designed to inform court staff and local organizations about emergency preparedness in the court. To sensitize external agencies and response partners to the importance of the judicial branch as a component of the government community, the court should consider forming a Judiciary Emergency Management Group composed of court leaders, state and local law enforcement officials, state emergency management officials, the bar association, and the public defender's office. This group should meet to plan collaboratively and thereafter meet periodically to review, update and practice the plan. This type of formalized outreach and awareness effort encourages communications under normal conditions and fosters relationships that become vital during response and recovery from a disaster.

Templates

In addition to the "Mission Essential Functions Template" referenced above, the reader may find the following templates useful:

- The Employee Directory Template at the Florida State Courts Emergency Preparedness Web site may be helpful for creating directories of contact information (http://www.flcourts.org/gen_public/emergency/bin/Employee%20Directory%20Template.pdf).
- *University of Virginia Library Disaster Preparedness and Recovery Plan*. Online March at <http://www2.lib.virginia.edu/preservation/disaster/disaster-plan-2005.pdf>,
- *COOP Plan Template Instructions*. Washington, DC: Federal Emergency Management Agency. http://www.fema.gov/pdf/about/org/ncp/coop_multi_year_plan_guide.pdf
- Emergency Preparedness Templates. Florida State Courts: http://www.flcourts.org/gen_public/emergency/templates.shtml
- <http://www.9-11summit.org>
- Memo of Understanding, whereby a county/parish will provide emergency space to a court. See template attached as Appendix F, modeled after a MOU utilized by the Juvenile Court in Jefferson Parish, Louisiana.

References/Resources

American University School of Public Affairs. “Guidelines for Pandemic Emergency Preparedness Planning: A Road Map for Courts.” 2007.

http://www.ojp.usdoj.gov/BJA/pandemic/Pandemic_Road_Map.pdf.

Bomb threat reporting forms are available on the Web site of the Department of Homeland Security.

http://www.dhs.gov/xlibrary/assets/ocso-bomb_threat_samepage-brochure.pdf

Note: Bomb threat reporting forms are also available from court security and emergency preparedness directors at state court administrative offices (AOC), *e.g.*, Florida, California.

Bureau of Justice Assistance and Center for Disease Control. “A Framework for Improving Cross-Sector Coordination for Emergency Preparedness and Response – Action Steps for Public Health, Law Enforcement, the Judiciary, and Corrections.” 2008.

<http://www2a.cdc.gov/phlp/EmergencyPrep.asp>.

Conference of Chief Judges. “Court Security Manual, State of Minnesota.”

<http://www.9-11summit.org/materials9-11/911/acrobat/27/P3&C10EmergencyPreparednessPlans/MinnesotaCtSecurityManual.pdf>.

Conference of State Court Administrators. “Position Paper on Emergency Preparedness in the State Courts.” Williamsburg, VA: National Center for State Courts. December 2006.

http://cosca.ncsc.dni.us/WhitePapers/EmergencyPreparednessStateCourts_Dec06.pdf.

COOP Planning. “Maintaining the Rule of Law – Planning for a Pandemic within an All-Hazards Context.” Williamsburg, VA: National Center for State Courts and State Justice Institute.

<http://riz0ep.rmxpres.com/riz0ep/viewer/?peid=38a092eb-9c0b-41b1-88eb-8e3e97dc0f55>.

National Association for Court Management. “Business Continuity Management Mini Guide.” 2006.

National Center for State Courts. “A Comprehensive Emergency Management Program: A Model for State and Territorial Courts.” 2007.

<http://www.ncsconline.org/emp/EMP%20PartI%20050307.pdf>.

National Center for State Courts. “Continuity of Court Operations: Steps for COOP Planning.” September, 2007.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=75>.

Ortwein, Carolyn E. “A Road Map for the Design and Implementation of a State Court Emergency Management Program.” Williamsburg, VA: National Center for State Courts.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=119>.

Siegal, Lawrence, Caroline S. Cooper and Allison L. Hastings. “Planning for Emergencies: Immediate Events and Their Aftermath: A Guideline for Local Courts.” Washington, DC: Justice Programs Office, School of Public Affairs American University. 2005.
<http://www1.spa.american.edu/justice/documents/2151.pdf>.

Supreme Court of Pennsylvania, Administrative Office of the Courts. “Courthouse Preparedness for Public Health Emergencies: Critical Issues for Bioterrorism/Biohazard Preparedness Planning.” Jan. 2006.
<http://www.prepare.pitt.edu/pdf/CourthousePrepBooklet.pdf>.

The Supreme Court of Ohio Advisory Committee on Court Security and Emergency Preparedness. “Court Continuity of Operations (COOP) Program Guide.” 2009.
<http://www.sconet.state.oh.us/Boards/courtSecurity/COOPGuide.pdf>.

University of Pittsburgh and Supreme Court of Pennsylvania. “Courthouse Preparedness for Public Health Emergencies – Critical Issues for Bioterrorism/Biohazard Preparedness Planning.” Jan 2006.
www.pacourts.us
<http://www.prepare.pitt.edu/pdf/CourthousePrepBooklet.pdf>.

Chapter 4: Disaster Recovery — Essential Elements of a Plan

It is well known that disasters and emergencies can occur without warning. A properly created and implemented disaster plan is the key to mitigating damage and facilitating a return to normal operations. A disaster has a broad impact, results in significant damage or loss, and requires the prolonged or extraordinary use of resources before normal operations can be resumed. An emergency is an adverse event that does not have widespread impact and does not require the use of extraordinary or prolonged resources to return things to normal. Proper and timely responses can prevent an emergency from turning into a disaster.

As is the case with most organizations today, data, in electronic as well as hard copy form, have become the “life blood” of courts. Managing data and files has become an essential court function. As discussed in the previous chapter, court operations face the risk of disruption that can be caused by many kinds of disasters or emergencies, both manmade and natural. When a disaster disrupts a court’s data system, the court will be hard pressed to discharge even its most basic and essential responsibilities. Therefore, courts must develop plans not only to prevent disruptions to data systems to the maximum extent feasible, but also to recover such systems as soon and as effectively as feasible after a significant disruption occurs. This chapter sets forth the basic steps for effective disaster recovery planning with respect to information management systems and for the preservation of hard copies of court records. (See Appendix D — “Model Disaster Recovery Plan Forms.”)

Step One – Leadership Commitment

Court leadership, both judges and administrators, need at the outset to understand the significance of disaster-recovery planning in the context of information management. This includes knowing at a fundamental level why it is so important and how it fits within the overall context of emergency preparedness as discussed in the previous chapter. Based on this fundamental understanding, court leadership must make a strong commitment to a vigorous planning methodology and to assigning the right number and mix of staff to implement the methodology successfully. Care must be taken to make

clear who has the responsibility and authority for disaster-recovery planning for both electronic and hard copies of the court's records. It is important that this responsibility not be assigned exclusively to the IT department. Users of technology within the courts have the most at stake in the continued availability of information, and, therefore, users of technology and those involved with the preservation of hard copies of records must play a significant role in planning and conducting information recovery.

Step Two – Risk Assessment

Risk assessment begins with an understanding of the court's data environment. What are the sources of data, and how are they made available to users. This is a relatively easy matter in the case of hard-copy data. Locations and subject contents of hard-copy files can be readily identified and located. Sources of electronic data and components for storage and delivery are more complex. Elements of electronic data systems to cover in a risk assessment include, by way of example, the following: desktop and laptop computers, servers, Web sites, email, local area networks, wide area networks, distributed systems, and mainframe systems.

Once the critical resources have been comprehensively identified, the next step is to determine the impact on court operations that would result from a material disruption in one or more of the IT system components. A determination needs to be made as to how significant each impact is and for how long it can be tolerated as well as how hard copies of records will be used. This analysis will inform recovery strategies and the priorities to be embedded in such strategies.

Assessing risks to establish a disaster recovery plan also involves looking at potential disasters that might affect some but not all components of a network or data center. A fire or earthquake might physically destroy records. Small-scale disasters are more frequent, such as power feeds or server crashes. Such small-scale disasters also have the potential to bring down courts' mission-critical functions.

Step Three – Disaster Recovery Plan

Developing a disaster recovery plan for IT and hard-copy systems will need to take into account the following factors:

1. The development of preventive strategies: While it may not be feasible to avoid altogether the disruptions caused by a disaster, the risks and/or consequences of such disruptions can be mitigated. Preventive strategies may include: emergency power supplies that can be sustained over a long period; sophisticated fire suppression systems; heat-resistant and waterproof containers for back-up electronic data and for vital hard-copy files; offsite storage of data, both electronic and hard-copy; and frequently scheduled data backup.
2. The development of recovery priorities: Regardless of steps taken to mitigate risks, disruptions can occur. When they do occur, a recovery plan must contain priorities to determine what the most important pieces to recover are and in what order they should be recovered. These priorities will be informed by the risk assessment the court has undertaken as a foundation for the recovery plan.
3. The development of recovery strategies: Once the priorities have been established, there needs to be a recovery strategy that addresses each priority. One essential recovery strategy that needs to be considered is the possible use of an alternative, offsite location at which to operate data systems during the course of the disruption. Size, location, compatibility, and availability are all factors that will need to be taken into account when considering an alternate site. Other strategies will, of course, need to consider restoration of the original site as soon as feasible, which will include issues such as equipment repair and/or replacement.
4. Clear assignment of responsibilities: It will need to be absolutely clear as to who has authority and responsibility for every material aspect of the disaster recovery plan. Disasters by their very nature breed confusion. Pre-planned clarity about who does what is essential for any realistic hope of recovery and restoration of operations.

5. Budget and resources: A disaster recovery plan needs to be realistic and have the staff and funds available to enable recovery to take place within reasonable timeframes.

Step Four – Testing

Waiting for a disaster to occur to see if a plan is effective is in and of itself a recipe for failure. Disaster recovery plans need to be thoroughly tested. The following areas should be included in a thorough test of the plan: system recovery on an alternative platform and alternate equipment; coordination among all those who have responsibility for recovery; internal and external connectivity; restoration of normal operations; and notification procedures. “Table top” exercises should be conducted where scenarios are tested in a classroom setting. More extensive function tests should also be conducted. Thorough and rigorous training on disaster recovery plans is an extremely critical part of plan testing.

Step Five – Plan Maintenance

The world of information technology is constantly changing. Accordingly, the disaster recovery plan needs to be continuously reviewed and updated as necessary. The plan should be thoroughly reviewed at least annually. More frequent reviews may be required to make sure that material changes in systems, equipment, and/or critical staff are appropriately reflected in the plan.

References/Resources:

“Disaster Recovery Planning for Courts: A Guide to Business Continuity Planning.”
Williamsburg, VA: National Association for Court Management.2000.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=0>

“Records and Document Recovery Techniques.” Florida State Library and Archives.
http://dlis.dos.state.fl.us/DisasterRecovery/records_and_document_recovery_techniques.pdf

Patterson, Pat. “Disaster Recovery Planning for Technology.” Court Information
Technology Officers Consortium: Technology Experience Bulletin, TEB: 2007-

02 (2007). <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=104>

Swanson, Marianne et al. "Contingency Planning Guide for Information Technology Systems." Washington, D.C.: National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. June 2002.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=115>

Diamond, Cindy. "Disaster Planning for Data Security." *Practice Innovations* 3, No. 1. March 2002.
<http://west.thomson.com/pdf/iii/PractInnovMar02.pdf>

U.S. Department of Commerce and National Institute of Standards and Technology. "Contingency Planning Guide for Information Technology Systems."
Note: This site contains detailed plan information and templates. Information in this chapter relies on a framework developed by this government agency.
<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>.

Chapter 5: Threat Assessment

It is incumbent upon all who work for the courts to ensure that justice is administered in an open, accessible, and safe manner. We live in a time when threats and acts of violence are directed toward judges as a result of their official duties. It is crucial that every threat directed against a judge be taken seriously and assessed. Courts should have in place a rigorous process to be followed when threats are received.

There is evidence to indicate that the number of threats against judicial officers has been growing in recent years. At the federal level, the U.S. Marshals Service reports that the number of threats against judges has almost doubled in five years, going from 674 in fiscal year (FY) 2003 to 1278 in FY 2008. At the state level, Frederick Calhoun and Stephen Weston, noted authors on the topic of threat assessment, have documented that nine local judges have been assassinated over the past 35 or so years, and identified another thirteen who have been physically assaulted. For example, in March 2005, an in-custody defendant in Georgia escaped by overpowering a deputy sheriff. In the process of escape, he managed to kill the judge and a court reporter. He then killed a deputy sheriff as well as a U.S. customs agent outside the courthouse.

Justice cannot be effectively dispensed when judges are faced with threats, so courts must have a comprehensive process in place to deal with them. The essential elements of such a process are discussed below. (For purposes of this discussion, the individual making the threat is referred to as the “suspect.” The judicial official against whom the threat is made is referred to as the “subject.”)

The Process of Threat Assessment

In order to be able to respond effectively to threats, it is imperative that courts have a solid, structured process in place. There are four essential steps to such a process:

1. Identifying the threat
2. Assessing the threat
3. Investigating the threat
4. Managing the threat

Identifying the Threat

A threat is an expression of intent to injure someone or damage something. A threat can be spoken, written, or symbolic (such as running one's finger across the throat, leading another to believe he or she is going to be killed). Determining that the communication is indeed a threat and not simply a statement of unhappiness is a critical first step in the process. Also, the process needs to identify the suspect and the subject and understand the relationship, if any, between the two.

Assessing the Threat

Once a threat has been identified, the next step is to assess how significant or serious the threat is. Upon receipt of a direct or implied threat against a member of the judiciary, a threat assessment should be conducted to determine the likelihood that the person making the threat will actually carry it out. To determine the risk associated with a specific threat, an assessment must be made of four characteristics relating to the suspect: intent, motive, opportunity, and ability. *Intent* is a purposeful course of action. *Motive* is the emotion, desire, psychological need, or similar impulse acting as an incitement to action. *Opportunity* is required for the threat to be enacted. *Ability* is having the resources and freedom to take the action.

Each of these four characteristics must be examined independently, then in combination with one another. For example, some suspects may be highly motivated but incapable of instigating an attack themselves because they are incarcerated. Other suspects can lack coherent motivation but truly intend harm. Of most concern are those suspects who possess strong intent, powerful motive, ample existing or created opportunities, and considerable ability.

The threat can be evaluated as to the degree of probability by the use of a number of tools, usually a matrix. More than one evaluation tool should be utilized. The use of several tools may be the main reason for further investigation, the involvement of professional psychologists, or the use of other law enforcement agencies. The following are four evaluation tools that are typically utilized:

- HRC, Version 20 – Historical Clinical Risk Management
- RAGE - V – Risk Assessment Guideline Elements for Violence, developed by the Association of Threat Assessment Professionals (ATAP)
- SARA, 2nd edition – Spousal Assault Risk Assessment Guide
- Violence Assessment Grid by James S. Cawood — addresses intelligence analysis and various levels of threat

There are two important factors to consider in assessing a threat against a judicial officer. First, judicial officers and court staff are good sources of significant intelligence about the suspect. Since virtually every threat emanates from a court case, the subject can provide important details about the case. Also, court records can be reviewed and may reveal clues about the issues and motive underlying the threat.

The second factor to bear in mind is that the suspect understands that the court has the potential to cause him harm. In the suspect's mind, the threat may be a defensive reaction prompted by some action by the court. The court may adversely affect the suspect's freedom or property. A restraining order can preclude contact with a spouse or children. Knowing the nature of the suspect's involvement with the court can shed important light on the suspect's motivation.

Investigating the Threat

Once the suspect has been identified and an assessment has been conducted, a determination needs to be made that the threat is serious enough to warrant further action. If so, then the next step in the investigation should be an interview with the suspect. This interview should take place at the suspect's home and be conducted by two trained investigators. Observing the contents of the house, the demeanor of the suspect, and the answers given will form the basis of a successful interview. Other occupants of the home should be observed carefully, not only to glean any possible corroborative factors regarding the investigation, but also to guard for possible threats to the investigators.

Those conducting the interview must possess enough information about the suspect, the threat, and the subject to ask pertinent questions and not risk antagonizing the suspect. During the interview, one of the two investigators should be looking for troublesome signs within the home. These include the presence of weapons or items

indicating an interest in weapons like gun magazines, hunting or gun competition trophies, news articles about the subject, and controversial books and writings.

Questions to pursue with the subject and the suspect in the course of the investigation include the following: What is the suspect's current employment status? How are the suspect's family relationships? Were prior threats made to the subject by the suspect? Did the suspect pursue or follow the subject? Does the suspect have a history of violence or a tendency toward emotional outbursts or rage? Is there evidence of prior mental illness or substance abuse? Does the suspect have possession of weapons? (A recent purchase of firearms escalates the threat.) Has the subject received any unsolicited correspondence or phone calls from the suspect? Does the subject believe the threat? Was the threat made in the presence of others? Is the threat detailed? Does the suspect have the means to carry it out?

If interviews of the suspect and subject, including answers to the above questions, raise sufficient red flags, then the following steps should be taken:

- If letters or notes from the suspect to the subject are discovered, these must be treated as crime scene evidence for possible DNA preservation.
- If a tape-answering device captured the threat, this too must be copied and preserved.
- A call-trace feature with the phone company should be installed for future documentation.
- A search warrant of the suspect's home, place of business, and motor vehicles should be obtained.
 - During the search, photos, journals, diaries, and other writings that describe the suspect's activities should be seized.
 - All computers must be taken.
 - Fingerprints and handwriting samples must be taken.
 - The National Crime Information Center (NCIC) or Targeted Violence Information Sharing System (TAVISS) must be searched to determine if the suspect is listed.
 - The suspect's photos must be shared with courthouse security and personnel for use during the investigation.

Managing the Threat

Once the assessment and investigation are complete and a determination is made that the subject has indeed been placed at material risk by the suspect, then preventive and/or management measures must be put in place. Responses can range from simply

holding a security briefing with the subject to more aggressive measures such as providing the subject with a security detail or even incarcerating the suspect.

Additional management strategies may include mental health commitments through the use of certified professionals. Long-term monitoring of the suspect, while costly, may be the only method to evaluate the danger he poses. Short-term monitoring is also part of the "watch and wait" strategy. Use of a Temporary Restraining Order (TRO) in certain circumstances may be appropriate. When using a TRO, the suspect must be personally advised of the conditions and consequences of violating the order.

All possible management strategies should be considered in light of the details of each case. The appropriate strategy is one that best fits the risks identified in the assessment and investigation. Some cases may only require that a briefing be given to subjects in order to increase their awareness and allow them to take some basic precautions. Other cases will require more aggressive strategies, up to and including incarcerating suspects.

Threat Assessment Training

In every court setting, there should be specifically assigned responsibility for handling threats, and the threat manager assigned this responsibility should be properly trained. The National Sheriffs' Association offers threat management training. The national chapter of the Association of Threat Assessment Professionals (ATAP) holds annual conventions, and many local ATAP chapters host one-day seminars. In addition, there is a growing library of research, articles, and books on contemporary threat management.

It is also important to train judicial officers and court staff on how to report threats. This will help give threat managers accurate information as quickly as possible. Although judges and senior staff need to be well trained in this regard, in fact the most likely sources for reporting threats are those on the "front line" such as receptionists, those working at court transaction counters or answering phones, mail handlers, and court security officers. These are the people who have the most contact with the public and are most likely to be aware of threats. Training these types of individuals on

reporting threat information will serve to make such information available in an accurate and timely fashion.

Communicating with Subjects

The subject of a threat should always be kept informed every time a threat is received. Communication with the subject should be ongoing throughout the stages of dealing with a threat. Not only are the judge and the judge's staff important sources of information, as indicated above, but ongoing communication will help calm the subject's concerns and provide assurance that the threat is taken seriously and that the response is being well managed.

Incident Tracking

Chapter 6 of this handbook will cover the topic of incident reporting. That topic interrelates with this topic of threat assessment. On the one hand, incident reports need to be regularly and systematically analyzed to see if they contain any indication of current possible threats against judicial officers. On the other hand, once a threat is received, the name of the suspect should be checked against information in incident reports on file to see what, if any, problematic behavior the suspect may have displayed in the past. These interrelationships can be best managed when one or both of the two systems (*i.e.*, threat assessment and incident reporting) are automated. But even a good index card system can be helpful in providing the necessary information.

Build Liaisons with Other Agencies

It is important to establish and maintain ongoing contacts with law enforcement agencies at the local, state, and national level. There is valuable intelligence that these agencies can provide about those who may pose a risk to judicial officers. Connecting the dots that may link individuals or incidents together can serve to identify threats in a more timely fashion and, thereby, minimize the risk that such threats pose. Toward this end, regular communication and coordination with other agencies can provide vital assistance to those with responsibility for the safety and security of judicial officers.

Conclusion

Threats made against judicial officers can seriously interfere with the business of the courts. While such threats cannot be eliminated, they can be effectively identified, assessed, investigated, and managed. A thorough, all-encompassing process for doing so can minimize the negative impact that threats have on the judicial system. A solid process can also potentially save the life of a judge.

References

Calhoun, Frederick S. and Stephen W. Weston. "Defusing the Risk to Judicial Officials: The Contemporary Threat Management Process." Alexandria, VA: *National Sheriffs' Association*. 2001.

<http://www.sheriffs.org/coda/CourtSecurityResources.asp>

Cawood, James S. "Enhanced Evidence Assessment and Management," *ASIS Seminar*. November 2007.

Clark, John F. "Protective Investigations Training Program." *U.S. Marshals Service*. August 2008.

Corcoran, Michael H., Ph.D. and James S. Cawood. "Violence Assessment and Intervention: The Practitioners Handbook." CRC Press LLC. 2003.

Judicial Council's Committee on Judicial Safety and Preparedness. "Unified Judicial System of Pennsylvania Court Safety & Security Manual." Administrative Office of Pennsylvania Courts. July 2005.

"Protecting Judicial Officials: Implementing Effective Threat Management Process." *Bureau of Justice Assistance Bulletin*. U.S. Department of Justice. June 2006.

<http://www.ncjrs.gov/pdffiles1/bja/213930.pdf>.

Yeschke, Charles L. "The Art of Investigative Interviewing: A Human Approach to Testimonial Evidence." *Butterworth-Heinemann*, an imprint of Elsevier Science. 2003.

For on-line information on the evaluation tools discussed in this chapter, see

HRC <http://www.violence-risk.com/hcr20annotated.pdf>

Rage V: <http://downloads.workplaceviolencenews.com/rage-v.pdf>

SARA: <http://www.violence-risk.com/risk/instruments.htm>

Violence Assessment Grid: <http://downloads.workplaceviolencenews.com/rage-v.pdf>

Chapter 6: Incident Reporting

Importance of Incident Reporting

A standardized mechanism for reporting security incidents is an extremely important aspect of a court's security program. As noted in responses to a CCJ/COSCA Committee on Court Security and Emergency Preparedness 2006 survey on incident reporting, a well-designed and managed incident reporting system can yield significant benefits in terms of court security. A good system will not only allow courts to respond more effectively to each security incident, it will also allow courts to analyze incidents in the aggregate, providing guidance for making improvements to overall security within the courthouse.

With respect to specific incidents, a good reporting system will let the appropriate officials know in a timely manner that a problem has occurred and will also provide essential information to allow the problem to be properly assessed, investigated, and handled. Court staff may observe something that appears problematic (for example, a door to a secure area that is propped open). Without an incident reporting system in place, this problem may go unreported and uncorrected. More serious and obvious incidents, such as someone pulling a gun outside a courtroom, will be dealt with even if there is no incident reporting system in place. But an incident reporting system will provide the information to respond to all incidents properly, whether obvious or subtle. It will provide information to enable authorities to investigate, apprehend, and convict perpetrators.

In the aggregate, data gathered from all security incidents over a span of time can provide invaluable information to those who have responsibility for courthouse security. This information can be periodically analyzed to identify patterns of conduct that reveal problematic security issues and vulnerabilities. Analyzing such information can provide decision-makers with a good basis for making informed decisions about overall improvements needed in courthouse security, for example, improving compliance and attitudes about the importance of court security. This analysis can also inform decisions about the allocation of existing resources for security and can be used to obtain additional funding to support the court's security needs.

Because of its intrinsic value and importance, an incident reporting mechanism is either mandated or strongly recommended in various state court security manuals or court directives. (For examples, see the manuals of Arizona, Arkansas, New Jersey, Pennsylvania, Virginia, and Wisconsin.) The value of an incident reporting system at the state and local levels would be immeasurably enhanced by the amalgamation of incident information at the national level. A national security summit, sponsored by the National Center for State Courts in 2005, acknowledged the importance of incident reporting in the context of a national database.

Two caveats are in order. First, an incident reporting program is no substitute for the need to report an incident to law enforcement promptly and directly. As circumstances dictate, law enforcement should be notified immediately about an incident, even before a report is prepared. Second, a security incident reporting program should not be confused with risk assessment. A security incident report is intended as prompt documentation of specifics of a security incident; its purpose is simply to create a record. Threat assessment, on the other hand, is a mechanism for protective intelligence. Threat assessment is a process of gathering and assessing information about individuals who may have the interest, motive, intention, and capability of harming persons or property at the courthouse. Threat assessments focus on vulnerability and interventions in order to manage the risks of targeted violence. Threat assessments require the organizational capacity to conduct sophisticated and systematic investigations.

Establishing an Incident Reporting System

A good incident reporting system begins with a good standardized form. Many states employ a paper process: the paper form is completed, perhaps reviewed, and then transmitted for filing and/or electronic input. Other states, such as Pennsylvania, have initiated an electronic process for the completion and transmittal of the incident report. The automated approach provides for greater speed in reporting and responding to incidents; and it facilitates creation of an easily searchable database of bulk information. In addition, such database information can also be easily and quickly shared among authorized users. But a court should not wait until an electronic system is established

before installing some level of incident reporting. It is more important to begin with a manual, hardcopy system rather than wait.

The standardized incident reporting form should be user-friendly to assist the preparer in promptly providing essential information with relatively little effort. A check box or checklist format can substantially simplify the process. As noted in NCSC's 2005 Security Summits I and II reports, it is advisable to identify only those pieces of information that are necessary. The tendency to collect too much information about an incident will often reduce "user friendliness" of a form and will create reluctance to use the form, which can result in the collection of only minimal information regarding incidents.

In the case of a bomb threat, for example, it is useful to have a specific format available at the desk of every staff person who receives phone calls from the public. (See Reference/Resources at the end of Chapter 3.) The form will serve to carefully guide the staff person into recording as much relevant and helpful information about the threat as possible.

There seem to be two schools of thought about verification and review of incident information. One approach is to have an eyewitness to an event promptly and independently fill out an incident report form and transmit it to a designated court administrator or law enforcement agent for inclusion in the paper-based repository or electronic database. In such circumstances, the form will be referred to the proper security official for follow-up, but there will be no official approval or editing of the form. This approach is based on the belief that it is better to capture more information quickly and directly from the person who witnessed the security event.

On the other hand, there are those who believe a security incident reporting form should be subject to oversight or approval before the information is officially transmitted for inclusion in the database and/or forwarded to a responsible official for follow-up. Upon receipt, the supervisor would review the document as soon as possible and, where necessary, follow up with the sender to offer assistance and ascertain that the information provided is understood and that no significant details have been omitted. This approach is based on the belief that it is better to restrict incident reporting to those persons who have received appropriate training regarding what incidents and related information

should be entered into the database. Proponents also contend that this approach promotes greater accuracy and consistency.

Regardless of the specific approach that is chosen, it is recommended that a trained court security officer or law enforcement supervisor should always be involved in any incident worth reporting to make sure information is documented and saved correctly.

There should also be a clear policy about who has access to the security incident reports and whether they will contain any personal identifiers. Given the sensitive nature of the information and its relevance to law enforcement, restricted access is advised.

Timely transmission of the reports is important. There should be a specified time from the occurrence and reporting of the incident to the completion and submission of an incident report. Also, recipients of the reports should be clearly identified. Appropriate recipients may include court administration (state and local), the local or state security committee, facility management, and law enforcement.

During the NCSC Security Summits I and II, there was discussion about the importance of providing feedback to the person who gave information about a security incident. Such feedback could include an acknowledgment that the information was received and how the security matter was addressed. New Jersey, for example, institutionalized an "acknowledgment and determination" process in its security incident reporting system. Also, in Pennsylvania, once a report is received, security staff will contact the individual who processes the report and determine if any assistance is needed.

All users of the incident form need instruction on the importance and mechanics of reporting. Although a user-friendly form can be substantially self-explanatory, assistance can promote the form's effectiveness. Pennsylvania, for example, provides court staff with an explanatory preface to the state's security manual's section on incident reporting, which contains a list of illustrative scenarios highlighting the nature of a reportable security incident. Educational security programs could include a segment on how to report a security incident. Training is especially important if reporting is done electronically.

In designing and implementing a security incident reporting process, it is important to invite and receive feedback from those with special interests and insight.

Collaboration with law enforcement, security management and prospective users is advisable. Several respondents to a 2005 survey suggested that an incident-reporting mechanism should be pilot-tested to assess potential problems or weaknesses. Pennsylvania, for example, conducted a trial run of its automated form with several counties before it was implemented statewide.

A security incident reporting form is intended to capture essential information for prompt transmission to management. Because of the important but limited use of the form, some states have created supplemental forms to serve distinct purposes. For example, special forms have been designed to guide a recipient in obtaining essential information in the event of a threat. (For example, see forms from New Mexico, "telephone threat form," and Wisconsin, "threat/security incident report.") Courts can also design daily summary logs regarding the confiscation of weapons and contraband at security control posts. This information can be especially helpful to document security needs and support funding requests. See Appendix E for Pennsylvania's Security Incident Fact Sheet.

The success of a security incident reporting system ultimately depends on compliance. Leadership again plays an important role. Court management (*e.g.*, presiding judge, court administrators, security management, and departmental supervisors) should stress the importance of this security initiative, exercise oversight, and consider appropriate incentives and enforcement mechanisms to maximize compliance. All levels of the judiciary should comply with security reporting requirements. If management does not view incident reporting as a serious endeavor, others will do the same.

Defining a Reportable Incident

The scope and clarity of definition will often determine a security incident reporting system's effectiveness. A "reportable incident" must be clear in both concept and application. A review of two very good report forms (from New Jersey and Pennsylvania) suggests that a relatively simple concept of a reportable incident can serve as a reliable springboard for a more detailed yet effective and user-friendly form. A reportable incident could be constructed on the following definitional foundation:

- **Acts of violence** (attempted or actual) to persons or property of the court system, to include, for example, assault, vandalism/damage to property, theft, disorderly conduct, and arson
- **Threats of violence** (oral or written), to include, for example, oral threat, written threat, bomb threat, mail threat, phone threat, or intimidation (*e.g.*, stalking)
- **Security implications** (acts that have an actual or potential impact on the safety of court personnel, the public, and the court's operations and facilities), for example, escape from custody, emergencies, contamination exposure, explosion, fire, weather, medical, suspicious activity, security breach, or security equipment malfunction

Pennsylvania's electronic-based form, for example, guides the user through a series of easy-to-identify categories with drop-down boxes in an attempt to identify with specificity the details of a court security incident.

Many states have incident reporting forms that are not structured to pre-identify the factual essentials of an incident; such forms defer to a generalized narrative summary of the event. This approach presents particular downsides: accuracy and completeness of information may be compromised, and *ad hoc*, non-structured reporting seriously complicates the ability to compile and analyze critically important information. A standardized reporting form avoids such deficiencies.

In comparing two structured and detailed forms from New Jersey and Pennsylvania, one can identify the following as recommended components of an incident report form:

1. Date of incident
2. Time of incident
3. General location of incident
4. Area of facility where incident occurred
5. Specific court division or unit in which incident occurred (*e.g.*, civil, family, etc.)
6. Connection with particular proceeding (caption, court term, and number)
7. Type of incident (*e.g.*, act of violence, threat of violence, security implication)
8. Weapon involved (used or displayed)
9. Contraband
10. Extent of injuries and/or property damage
11. Identification of who was involved in incident
12. Action taken/resolution
13. Brief description of incident/summary of facts
14. Identification of preparer's name and position, including signature
15. Date of report
16. Identification of supervisor (if review or approval is required)

Finally, there is an ongoing effort by the NCSC and others to create a model standardized incident reporting form that will be used by all state courts. Such a model form would facilitate and improve statistical reporting on security nationwide.

References/Resources

Note: Incident reporting forms for Pennsylvania and New Jersey Administrative Office of Courts are available on their Web sites or by contacting the states' judicial department directors of court security.

Chapter 7: Funding for Court Security

Court security is a distinct and essential part of court operations. Security helps guaranty access to the courts. For budget purposes, courts need to include the cost of security as a necessary operational expense. When facing difficult economic times, budgetary support for court security at the state and local level will necessarily be incremental. Some essential components of court security, such as the creation of a security committee and the development of policies and procedures, require little or no cost. However, as indicated in other chapters of this handbook, equipment and law enforcement personnel required for court security can be expensive.

Sustained communication and alliances with other interested stakeholders can be of great use in funding court security. This notion is discussed in Chapter 8 of this handbook. Adequate funding remains a challenge. While some assistance may eventually come from the federal level, court security ultimately remains a state and local responsibility as well as a potential liability.

Federal Funding for Court Security

At this time, there appears to be little in the way of direct federal funding for state courts. State and local courts have been unable to apply directly for resources. In most cases, those federal funds that are available flow from the Department of Justice or Department of Homeland Security and are dispersed to the states. On the state level, an administrative agency or official then can disperse the funds. Unfortunately, this often creates competition between the executive and judicial branches for funding.¹⁴ There have been attempts to lobby Congress to allow state courts to apply for the federal funds directly. To date, these efforts have not been successful.

Nevertheless, organizations such as the Conference of State Court Administrators (COSCA) have continued to lobby Congress for funding for court security issues. Chief Judge Robert Bell, in his position as president of the Conference of Chief Justices (CCJ), spoke to the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security and urged the members to create a new federal grant program specifically

¹⁴ Casey, Pamela. *A National Strategic Plan for Judicial Branch Security*. p. 8 (2006).

targeted to assess and enhance state court security, ensure that state and local courts are eligible to apply directly for discretionary federal funding, and ensure that state courts are included in the planning for disbursement of federal funding administered by state executive agencies.¹⁵

Mary McQueen, president of the National Center for State Courts, testified to a House committee on the importance of a Threat Assessment Database and a mechanism to ensure uniform collection of data and data-sharing among states. She also asked the committee to consider funding for the NICS Improvement Act, which would provide grants to state and local courts in reporting mandatory data to the National Instant Criminal Background Check System (NICS).¹⁶ Although the House did not include the requested funding, its report accompanying the bill urged the Department of Justice's Bureau of Justice Assistance to devote resources to the problem of courthouse violence.

State Funding for Court Security

Funding for security measures in the state and local courts is generally provided by several methods: court fees and assessments, direct appropriation by the legislature, and — in some cases — donations by interested parties. Court security funding can either be under direct control of a court or the control of others.¹⁷ These “others” who provide grants to courts may be the state supreme court or the state court administrator's office.

One issue regarding court security funding is that it is often looked upon as a budget line from which money can be taken should a state's fiscal situation worsen. In two instances below, there are efforts to take monies from the court security fund (for unspecified reasons). California has recommended creating a court security budget line item and requiring that allocations be used only for security efforts and the unused funds be allowed to roll over to the next year.¹⁸

¹⁵ Bell, Robert W. *Written Testimony on Improving Security of Our State Courts*. 7 (2007).

¹⁶ Testimony by Mary McQueen to the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies. April 2, 2009.

¹⁷ Raftery, William. *Gavel to Gavel*. February 15, 2007.

¹⁸ Judicial Council of California. *Recommendations on Trial Court Security Funding Standards and Methodology*. p. 3.

A LEXIS search of all state codes, state constitutions, court rules, Advanced Legislative Service (ALS), and legal periodicals reveals how the following states fund their court security efforts:

Arkansas

Arkansas has created a central fund for court security, which is distributed by the Administrative Office of the Courts.¹⁹

California

California assesses a \$20 fee for any criminal conviction, which is disbursed into the security fund for state courts.

Colorado

Colorado created a court security cash fund commission and assesses a \$5 fee on most civil actions, criminal convictions, probate filings, and traffic infractions.²⁰

*Note: There have been attempts to divert monies from this fund to the general fund for unspecified reasons.*²¹

Delaware

Delaware imposes court assessment fees of up to \$10 on civil filings and each criminal, traffic, or delinquency charge where there is a conviction or finding of delinquency or responsibility.²² These monies are then deposited in a court security fund and maintained separately from the general fund.

Illinois

Illinois allows jurisdictions to impose a court services fee for civil actions and in convictions of criminal, local or county ordinance, traffic, and conservation cases.²³

Maine

Maine created a courthouse security fund under Supreme Judicial Court control. It consists of all money appropriated or allocated for inclusion in the fund from whatever the source.²⁴

Mississippi

Mississippi has created a state court security systems fund, and monies deposited into the fund are used by the Administrative Office of the Courts for court security.²⁵

¹⁹ For the coming year, \$361,043.00 has been appropriated; 2009 Ark. ALS 1499.

²⁰ C.R.S. 13-1-201 (2008); C.R.S. 13-1-204 (2008).

²¹ 2009 Colo. SB 208; 2009 Colo. SB 279.

²² 10 Del. C. § 8505 (2009).

²³ 55 ILCS 5/5-1103 (2009).

²⁴ 4 M.R.S. § 58 (2008).

²⁵ Miss. Code Ann. § 37-26-9 (2008).

Montana

Montana courts apparently receive funding from the legislature. Chief Justice Mike McGrath reported that recently \$300,000 was appropriated for courtrooms in Montana.²⁶

Nevada

There is proposed legislation in Nevada allowing a filing fee of not more than \$20 to be assessed for court security efforts.²⁷

New Mexico

County commissioners are responsible for court security.²⁸

Oklahoma

Oklahoma assesses a courthouse security fee of \$10 for criminal actions.²⁹

Oregon

Oregon's counties maintain a court security account for providing security services.³⁰ Courts' fees are assessed in a range of \$3 - \$7.³¹

Note: There has been an attempt to divert funds from the State Courts Facilities Security Account to the general fund for some unspecified reason.³²

Pennsylvania

Since 2004, Pennsylvania has dedicated a separate line item in the state's judicial budget to support court security (programs, equipment, services, and training).

Tennessee

Tennessee assesses a \$2 fee on criminal cases to be deposited into the county general fund for courtroom security.³³

²⁶ 34 *Montana Lawyer* 18 (November 2008).

²⁷ 2009 Nev. ALS 443.

²⁸ N.M. Stat. Ann. § 4-41-16 (2008).

²⁹ 28 O.S. § 153(E).

³⁰ ORS § 1.182 (2007).

³¹ ORS § 137.309 (2007).

³² 2009 Ore. SB 581.

³³ Tenn. Code Ann. § 8-21-401 (2009).

Texas

Texas assesses a court fee of from \$3 to \$5, depending on the criminal offense, for court security purposes.³⁴ The county commissioners can authorize civil filing fees of from \$1 to \$5 (\$20 in Webb County) for court security purposes.³⁵

Utah

Utah has created a restricted account within the general fund known as the Court Security Account.³⁶ A security surcharge of \$25 is assessed in all courts of record on all criminal convictions and juvenile delinquency judgments.³⁷ In addition to any fine, penalty, forfeiture, or other surcharge, a security surcharge of \$32 shall be assessed on all convictions for offenses listed in the uniform bail schedule adopted by the Judicial Council, and moving traffic violations, of which 25 percent of that amount is to be deposited into the Court Security Account.³⁸ The Court Security Account also gets \$15 of civil filing fees.³⁹

*Note: A Recent Utah House bill is trying to increase the fee amount.*⁴⁰

Virginia

Any county or city, through its governing body, may assess a sum not in excess of \$10 as part of the costs in each criminal or traffic case in its district or circuit court in which the defendant is convicted of a violation of any statute or ordinance.⁴¹

West Virginia

West Virginia has created a special revenue fund known as the Court Security Fund, within the Department of Military Affairs and Public Safety, which is chaired, by statute, by the supreme court administrator. The Court Security Fund may receive any gifts, grants, contributions, or other money from any source that is specifically designated for deposit in the fund.⁴² West Virginia assesses \$5 on each civil filing fee to be deposited in the Court Security Fund⁴³ and \$5 on each criminal case.⁴⁴

³⁴ Tex. Code Crim. Proc. art. 102.017 (2009).

³⁵ Tex. Gov't Code § 101.0615 (2007).

³⁶ Utah Code Ann. § 78A-2-602 (2008).

³⁷ Utah Code Ann. § 78A-2-601 (2008).

³⁸ Utah Code Ann. § 78A-2-601 (2008).

³⁹ Utah Code Ann. § 78A-2-301 (2008).

⁴⁰ 2009 Ut. HB 455.

⁴¹ Va. Code Ann. § 53.1-120 (2009).

⁴² W. Va. Code § 51-3-14 (2008).

⁴³ W. Va. Code § 50-3-1 (2008).

⁴⁴ W. Va. Code § 50-3-2 (2008).

For states not listed above, general court security funding is part of the general judicial appropriation by the legislature. In New York, for example, funds for court security are allocated in the proposed annual judiciary budget request.⁴⁵

Donations by Interested Parties

In a few cases, courts have received funding from interested parties. A 1997 survey by the American Judges Association (AJA) listed bar associations as an unusual source of funding.⁴⁶ Kansas courts have received monies from the Kansas Highway Patrol to enhance physical security.⁴⁷

Recent Attempts at Funding

Montana

SB 191 – Would provide funding for court security, sponsored by Sen. Larry Jent (D), an attorney from Bozeman: This bill would require all courts of original jurisdiction to impose a user surcharge in criminal, civil, and probate cases. The surcharge must then be used by local governments for the payment of costs for court security needs. The bill was indefinitely postponed on the Senate floor and is probably dead.

<http://data.opi.mt.gov/bills/2009/billpdf/SB0191.pdf>

References

Pines, Zygmunt. “Prudent Risk Management: A Court Administrator’s View.” *Justice System Journal*. p. 58-61. 2007.
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=85>.

⁴⁵ New York State Unified Court System. “The Task Force on Court Security: Report to the Chief Judge and Chief Administrative Judge.” p. 4 (2005).

⁴⁶ American Judges Association, *Court Security Survey Report*. 1997. Available at <http://aja.ncsc.dni.us/Old%20Website/Ctsecurity.html>

⁴⁷ From chart in *National Summit on Court Safety and Security Follow-Up Meeting Participant Book* (2005).

Chapter 8: Security Equipment and Costs

Availability and cost of security technology and equipment – essential court security tools – are major considerations for those responsible for ensuring a safe, secure court environment. Having the necessary security equipment with appropriate state-of-the-art technology, along with the training necessary to operate that equipment, will serve the court family and the public well by minimizing opportunities for violence. This chapter describes the essential technology and equipment needed in the provision of basic court security. It also provides general information on costs. It is important to note that the price of equipment will change over time and is subject to state bids and the selection of vendors. For example, costs will ultimately depend in most cases on the bid awards that court systems are able to make in response to requests for proposals (RFPs). It is important to note that the Committee does not endorse or recommend the purchase of any specific court security or emergency preparedness technology or equipment by specific vendors. State judicial departments are encouraged to contact their authorized purchasing department or agent.

Access Control: Hand Wand, Magnetometer, and X-ray Machine

Access control is the essential first step in providing a safe environment for the courthouse. The major objective of access control is to prevent people from bringing weapons into the building. A weapon is considered any device that could be used to harm another; this includes anything from a gun to a knife to a knitting needle. The security equipment used at the screening station at the entrance to the courthouse provides the first line of defense in the effort to prevent the introduction of weapons into the courthouse.

The most basic screening device required is a handheld metal detector (also referred to as a hand wand), which is used to scan a person, a handbag, and/or briefcase to detect concealed metal. Often this hand wand is used in conjunction with a walk-through metal detector. Most handheld devices sold today are self-calibrating, meaning that they automatically adjust the sensitivity level when in use. These hand wands are durable and rugged enough to be dropped and still perform efficiently. No special tools

are required to operate this device, and the convenient simplicity provides for easy operation. The hand wand has become a vital tool in successful screening processes at courthouse entrances around the country. The cost of a handheld metal detector is about \$150 to \$300 for the most popular brands. These battery-operated units typically have a long life and in most cases come with a full two-year warranty.

The next basic piece of equipment in access screening is a walk-through metal detector known as a magnetometer. Magnetometers fall into two categories: single-zone detection and multi-zone detection. When a person walks through a magnetometer with a concealed weapon located at his ankle, both the single- and multi-zone magnetometers will detect the weapon. The difference between the two is that the multi-zone detector will pinpoint the location of the weapon on either the individual's left or right side. More advanced multi-zone detectors will also pinpoint the specific location from head to toe. Pinpointing the location of the weapon quickly is important so that court security officers can respond swiftly. When scanning a large volume of individuals, a multi-zone magnetometer will facilitate processing the public through the screening station more quickly.

Modern walk-through magnetometers are easy to set up and operate. Most units come with a detailed manual and instructions. Digital electronics are easily adjusted through a touch pad and LCD display. The magnetometers come with factory preset programs, but they can also be adjusted for specific locations or for the type of object screening officers are trying to detect. Based on the level of sensitivity selected, the detector can be adjusted to locate various targets.

Controlling the flow of traffic is an important consideration when setting up magnetometers in screening stations. It is a good idea to have a basket or tray next to the magnetometer where individuals can place metal objects, because it is important that watches, coins, keys, and other large metal objects are removed before walking through the detector. The better organized the screening station is, the better the through-put will be.

The cost of walk-through magnetometers for court operations varies from a low of \$2,000 up to \$12,000 or more for the most advanced models. It is important to note that buying in bulk can save a significant amount of money when acquiring magnetometers.

Courthouse screening stations should also be equipped with x-ray machines in order to detect weapons and explosives in a non-intrusive way. The machine consists of a generator that sends x-ray beams or radiation into the object being screened. These x-ray beams are passed through a processor, creating an image on a computer screen. The court security officer assigned to the computer reviews the images and, with proper training, will be able to identify dangerous objects entering the courthouse. The x-ray machine should be inspected annually and tested for leakage. Note that the radiation from one of these machines is low in dosage and safe to be near. The median cost of a standard x-ray screening machine for a courthouse is approximately \$32,000. Again, bulk purchasing will have a dramatic effect on pricing.

There is new technology in x-ray machines, but it comes with some controversy. This new technology is called a backscatter x-ray scanner. In contrast to the traditional x-ray machine which detects hard and soft materials by the variation in transmission through the target, backscatter x-ray detects the radiation that comes back from the target. It has potential applications in almost every situation in which non-destructive examination is required, but only one side is available for examination. One application currently under testing is a security scan of airline passengers. The technology has been proposed as an alternative to personal searches at airports and other security checkpoints, since it can easily penetrate clothing and reveal concealed weapons. However, it raises privacy concerns in that it appears to screeners essentially as a nude picture of the subject, and it may allow screeners access to otherwise confidential medical information.

The American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center are opposed to this use of the backscatter technology. The ACLU refers to backscatter x-rays as a "virtual strip search." The Transportation Security Administration (TSA) announced in a November 2007 press release that to date, 79 percent of the public has opted to try backscatter over the traditional pat-down in secondary screening. The TSA began using backscatter x-rays in February 2007.

Duress Alarms

Duress or panic alarms are essential components of any effective court security program. A duress alarm button may be portable or may be mounted in a strategically

pre-determined location such as a judge's bench, chambers, or a public transaction counter. In a duress situation, the judge or staff member depresses a hidden button, sending a silent, remote signal for help to emergency responders. A duress alarm system should alert court security officers or local police to the location of the area needing assistance. It is the primary technology used in courthouses across the country today to alert first responders.

There are two basic types of duress alarm systems on the market today. The first is the hard-wired alarm that has a permanent mount under a desk or counter. The other, newer type is the wireless system that runs through a radio frequency. This system alerts pagers and two-way radios used by security officers that an alarm has been activated. A new system uses a GPS satellite to locate the activated duress alarm. New technology is constantly improving this type of system.

The hard-wired duress alarm system has some weaknesses that need to be considered. If the duress alarm is tied to a busy server on the computer mainframe, a delay could result. The security department must test the system frequently by activating each alarm to be sure it is working properly. Another problem is that the duress alarm can be activated inadvertently, causing a false alarm situation. The more this happens, the less likely an alarm will be treated as a genuine emergency in the future.

Costs of duress alarm systems vary depending on several factors, including size of the courthouse (or multiple courthouses) tied into the system and how many buttons need to be wired to the control panel. A large courthouse could be wired for approximately \$10,000, including the control panel and enough duress alarms for courtrooms, chambers, and public counters. A panel can cost \$1,000, and each emergency button costs approximately \$200. A competitive bidding process (RFP) is advised to receive the best system at the best price.

Closed-Circuit Television System

No court security program would be complete without an integrated closed-circuit television (CCTV) system with digital recording capabilities and a security control room monitoring the cameras throughout the courthouse. A CCTV system is the strategic placement of video cameras that send images to monitors and recording devices for viewing and later recall. A CCTV system should be installed in a courthouse setting to monitor areas within the court as well as surrounding areas that may be trouble spots. These cameras act as a deterrent to crime, and the images produced can be used as evidence when reconstructing an incident or crime on the premises. CCTV systems have come a long way in a few short years, going from black-and-white, fixed-position images, to full-color, tilt/pan/zoom capabilities. These new systems can recall video from archived digital files, providing the opportunity to “go back in time.” A digital video recorder (DVR), as part of an integrated CCTV system, will provide 14 days of high-resolution recording. This gives authorities time to compile evidence for a criminal charge, if necessary.

Determining the cost of a CCTV system for a courthouse or court complex can be quite detailed. Electrical wiring and necessary components to a compatible control room can be very expensive indeed. The equipment is only part of the overall expense. Including top of the line tilt/pan/zoom color cameras with mounting equipment, multiplexers, and monitors, a set of 16 units will cost between \$20,000 and \$30,000, excluding labor costs. In all cases, a detailed RFP should be issued with no less than three reputable quotes from established vendors with impeccable security credentials for their companies and their individual employees.

Intrusion Alarm System

An intrusion alarm system consists of panels, signaling components, and sensors that can detect the following: unauthorized movements, forced opening of doors and windows, breaking glass, smoke, fire, and leakage of water or chemicals. A breach in courthouse security can happen anytime — day or night. Installation of an intrusion alarm system creates a much safer environment. The system’s brain is the control panel,

ideally located at a security command and control center. Various kinds of sensors are connected to the control panel from locations around the court perimeter.

There are alarm sensors for two basic types of protection: perimeter and interior. Perimeter protection sensors are located at the vulnerable entry points of the court such as doors and accessible windows. These perimeter protection sensors include magnetic contacts and glass break sensors. Interior sensors detect motion inside the courthouse. One example is the passive infrared detector (PIR), which detects motion through body heat. Smoke and fire detectors are other types of interior protection, usually located high on inside walls or ceilings.

When a sensor reports a signal to the control panel, it analyzes the report to determine which sensor is reporting and whether the problem is an intruder, fire, or an emergency of some other kind. After this quick analysis, the control panel can sound an alarm or siren alerting security officers that a problem has occurred. The unit can activate lights and can alert a 24-hour monitoring service, which can then verify the alarm and dispatch police, fire, or medical help, as necessary. Typically, the monitoring service is notified by a digital message sent over regular telephone lines.

Determining the project cost for a complete integrated intrusion alarm system for a courthouse or court complex can be a challenge, but it is well worth the effort for a good security program. Costs will encompass all the components, from the control panel to each sensor or detector at entry points as well as the electrical wiring necessary to bring everything together in a comprehensive security command and control center for monitoring. As with every major purchase, the quality of the equipment and the volume of work required to complete the system should be put into an RFP for qualified vendors.

Access Cards

The next process in enhancing courthouse security is the purchase of a computerized, identification-card access control system. A card access system is vital to providing a secure courthouse for judges, staff, and the public. Restricting access to the courthouse at specific entry points to authorized people only is the purpose of this technology. A well-managed card access system will virtually eliminate the need for keys, which can be lost, stolen, or copied. Keypad systems are less effective because

employees forget the combination or pass it on to someone else, causing a security breach. One of the major benefits of the computerized card system is that the software tracks time and entry points of users, leaving a record for later review.

The card access control system has three main components: the access card itself, a proximity reader and locking mechanism for entry points, and the computer system software. Using the access card provides several benefits, most notably access levels. This means that the administrator controls who can go through what door at what time. Some courts use the services of outside contractors where this feature would enhance court security. Another benefit is that an access card can be instantly turned off or on, immediately providing or denying access.

To determine the cost of a complete system, it is necessary to identify how many doors, garage openings, and parking gates need to be included. The cost of a complete system includes a full accounting of all doors, garage openings, and parking gates that must be included in the system. Costs are affected by the number of employees and visitors who require access cards on a daily basis, the manner in which the system is managed, the process by which cards are issued, decisions about who will monitor access, and other local needs. A comprehensive integrated access control system median price is estimated at \$2,500 per access point, not including cards or installation. Again, many quality providers for this service exist, and an RFP with a minimum of three vendors is recommended.

Command and Control Center

The command and control concept is about understanding what is happening, at any given time, anywhere in the courthouse. When designed to work with the specific needs of command and control operations, an integrated electronic security system becomes a valuable component that integrates diverse and disparate security equipment and relieves operational burdens from personnel. A single cohesive security network enables information to be retrieved, decisions to be made, and the investment to be leveraged to the fullest. A well-constructed and well-staffed control center will serve to meet daily operational challenges necessary for a safe working environment in the courthouse.

The security command and control center for court operations provides a central hub, usually a room on site dedicated to this security function, where the electronic systems described above are monitored. Information gathered there can be used to handle many challenges that a court faces, including fires, vandalism, burglary, robbery, loitering, high-profile trials, inclement weather events, and power outages. Rather than providing bits and pieces of information, electronic security can be designed to provide a total picture within the court facility.

In order to get the most from a security system, it needs to be used properly. A comprehensive and ongoing training program is fundamental to meeting this challenge.

Other Security Equipment

There are other equipment components to a comprehensive court security program that are worthy of consideration. Examples of these items include

- **Security lighting and fencing.** The use of high-intensity sodium lights can be a very cost-effective security measure. There should be sufficient lighting around the perimeter of court buildings and in parking lots in order to avoid shadows and allow for CCTV cameras to capture images. Fencing should be of sufficiently strong material, appropriate in height, and angled outward at the top to minimize the risk of someone climbing over the fence.
- **Protective barriers for public counters.** These should be made of Plexiglass™-type material or shatter-resistant glass. The bottom of the glass should be no higher than 24 inches above the countertop.
- **Bollards to prevent vehicle entry crashes.** Bollards must be able to stop a 4,000-pound vehicle at 30 mph. They should consist of eight-inch diameter, stainless-steel pipe core, with 4,000 ksi concrete fill. They should have a minimum height above and below grade of three feet and provide 20-inch cross dowels that protrude a minimum of six inches on either side of the bollard. Maximum spacing between bollards is four feet, center to center.
- **Ballistic material for judges' benches.** Opaque, ballistic-resistant material that meets UL Standard 752 Level III should be installed behind the vertical surfaces on the three sides of the bench visible to the public.

All of the equipment discussed in this chapter is intended to protect people and property, while at the same time provide public access to an open judiciary. This balance is not easy to maintain. A security industry resource for equipment and related costs is the *Security Industry Buyers Guide*, which is published annually and available online at www.sibgonline.com. It is the most current, comprehensive database of security

products and services in the industry. Comprising more than 3,000 manufacturers and suppliers of security products and services, the SIBG fully categorizes the available resources of the security industry from the most elemental tools to its most advanced technology.

References

American Society for Industrial Security

<http://www.asisoline.org/>.

Guidelines for Implementing Best Practices in Court Building Security - Costs, Priorities, Funding Strategies, and Accountability: A Paper by the National Center for State Courts. Funded by the State Justice Institute, Grant Number SJI-09-P-125

Chapter 9: Resources/Partnerships

While in the final analysis courts may have ultimate responsibility for courthouse security, it is a responsibility that cannot be successfully discharged by courts alone. Courts on their own do not have the capacity or resources to address their own security needs fully. Cooperation and coordination with a host of other organizations are imperative. Other organizations have a shared interest in courthouse security, or they have the capacity to provide resources to help make courts more secure, or they have both.

According to Zygmunt Pines, state court administrator for Pennsylvania and co-chair of the CCJ/COSCA Committee on Court Security, “We need to build a culture of collaboration that will create a mutually supportive network of information and assistance. From my vantage point, collaboration needs to take place on many levels.”

- **Local** – within the facility itself, with broadly representative standing committees on security and with law enforcement, executive, and legislative leaders
- **Regional** – with colleagues and partners who can provide guidance on common issues or support in the event of a debilitating incident
- **State** – with court leadership, executive-level committees on security and disaster planning, the legislature, and state police
- **National** – with the Department of Homeland Security, Congress, and various associations and organizations such as the National Sheriffs' Association and National Center for State Courts

Partners for Collaboration

The following are key entities courts should look to for assistance and cooperation in the daunting and vital challenge of making court buildings as secure as they can possibly be.

U.S. Marshals Service

In fiscal year 2008, the U.S. Marshals Service (USMS) established a National Center for Judicial Security (NCJS) that is operated, staffed, and managed by employees and contractor staff of the USMS Judicial Security Division. The NCJS provides educational, operational, and technical functions that are designed to serve various needs of a national, and in some cases, an international constituency. The NCJS also provides a

wide range of support and services to municipal, city, county, state, federal, and international jurisdictions related to the security operations of their respective court systems and protection of members of the judiciary and extended court family.

The National Center for Judicial Security Fellowship Program (NCJSFP) is designed to afford a professional opportunity to state, local, and international court security managers to train and serve with USMS counterparts in all facets of the USMS program and experience high-level executive protection and security operations in the Fortune 1000 private sector. The Judicial Security Fellow will participate in joint training with court administrators at the National Center for State Courts in Williamsburg, Virginia, in areas such as coordination of public and media relations in high-visibility trials, coordinated approaches to policy and procedures implementation, consolidated training for clerical staff in security awareness and response procedures, and working with the judiciary.

National Sheriffs' Association – Court Officers Association

The National Sheriffs' Association is dedicated to court security training and has long provided education for maintaining courthouse security and guarding the courthouse workgroup, citizens, and users of the judicial system. Some of the training provides an introduction to contemporary concepts and law enforcement strategies related to courthouse and courtroom security. Topics include understanding the need for vulnerability assessment, knowing current courtroom security standards of practice, understanding the need for professional awareness, understanding the basic dynamics and operations needed in planning a high-risk/high-profile trial, and understanding the basic need for advanced planning for emergency events.

Local Police/Sheriffs/Security Personnel

Local police and sheriffs should be part of any court security efforts. It is essential that those involved in court security reach out beyond the courthouse and maintain contact with other security and law enforcement personnel to gather information and assess threats to court security. Information from various resources can be pieced together and often reveal relationships and behaviors of subjects who may be of concern

to courts. For example, after September 11, 2001, the New York judiciary worked with various partners to assist families and provide court-related information to the public. It also designated one or more officials to work full-time at the New York City Office of Emergency Management and with the New York City Court — Terrorism Task Force. In some states, the need for additional personnel is recognized by state law. For example, Kentucky provides for compensation of local police when used for court security.

Local Government Officials

Quite often, courts are left out of plans for security and emergency preparedness although they will typically play a major role when events take place. The chief justice and state court administrator can stress the importance of the courts to local government officials and leaders to ensure courts are included in any emergency or security plan. Since in many jurisdictions local government officials may be responsible for funding the courts and related security measures, it is essential that a close working relationship be established.

Local Bar Associations

The local bar association is often a good resource for court security. As with judges and the public, it is important that the local bar be aware of and on board with court security. In many cases, members of the bar can provide lobbying efforts for court security measures. One example of local bar association cooperation is the Allegheny Bar Association, which has raised funds and created a political action group to lobby lawmakers for issues of importance to the bar. Among the priorities is supporting the continued funding of the Allegheny County (Pennsylvania) Court of Common Pleas, which will enable Allegheny County to improve court facilities and provide adequate security for judges, court support staff, attorneys, and the general public.

Example of Collaboration – Department of Homeland Security

The Web site “Lessons Learned Information Sharing” (www.LLIS.gov) is the national network of lessons learned, best practices, innovative ideas, and preparedness information for homeland security and emergency response professionals. By facilitating the sharing of knowledge, LLIS.gov enhances the nation's ability to prepare for and respond to terrorism, natural disasters, and other incidents. The Web site is not only a repository for information but also a network that enables homeland security and emergency response professionals from across the country to share knowledge and expertise in a secure, online environment.

Positioning Courts to Facilitate Collaboration

In order to be well-positioned to reach out to potential security partners effectively, court leadership should take care to make sure that the court itself has its security responsibilities properly organized. Key to this is to have one or more court security committees.

Ideally, a court security committee should be chaired by the presiding judge and consist of stakeholders with an interest in or responsibility for court building security. Such stakeholders could include representatives of the following: other judges in the court system, court administration, court security department, local law enforcement (*e.g.*, sheriff, police department), the county administration, the district attorney’s office, the bar, and the public.

The committee should meet regularly and encourage candid discussion of security concerns among its members. Subcommittees can be established to study and assess various areas of court security and report back to the committee. Examples of such issues assigned to subcommittees might include policies and procedures, access control, prisoner transport, facilities, funding, incident and contraband analysis and reporting, screening, and training.

Cooperation of local judges and the community is important for a comprehensive court security plan. Often, those responsible for court security may have to advocate for new or stricter security measures. Since, in many areas, courts have been traditionally open and used for numerous non-judicial events and occasions (such as weddings, school

events, community meetings, etc.), it may take some effort to change attitudes concerning security. A rural sheriff once explained the effect of public attitude in his community where everyone knew everyone by name. He believed that he could probably impose some stricter security, but there would probably be an acceptable limit to what he could do. Collaboration and communication with stakeholders and the court's community are important in fostering awareness and promoting change.

References/Resources

Allegheny County Bar Association. "9 Lawyers." *The Bar Journal*. 2007.

Bureau of Justice Assistance and Center for Disease Control. "A Framework for Improving Cross-Sector Coordination for Emergency Preparedness and Response – Action Steps for Public Health, Law Enforcement, the Judiciary, and Corrections." July 2008.

<http://www2a.cdc.gov/phlp/EmergencyPrep.asp>.

Campbell, Colin F. and Marcus W. Reinkensmeyer. "The Court Security Challenge: A Judicial Leadership Perspective." *Justice System Journal*, Vol. 28, No. 1 p. 51. 2007.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=87>.

Casey, Pamela. "A National Strategic Plan for Judicial Branch Security: Prepared for the National Center for State Courts and the National Sheriffs' Association." Williamsburg, VA: National Center for State Courts. 2006.

http://solutions.ncsconline.org/Recommended_strategies_Appendices_Final_Report_2-7-061.pdf.

Colorado State Court Administrator's Office. "Colorado Courthouse Security Resource Guide." 2008.

http://www.courts.state.co.us/userfiles/File/Administration/Financial_Services/Court_Security_Resource_Guide.pdf.

Conference of State Court Administrators. "Position Paper on Emergency Preparedness in the State Courts." p. 9. 2006.

http://cosca.ncsc.dni.us/WhitePapers/EmergencyPreparednessStateCourts_Dec06.pdf.

Kentucky Supreme Court. "KRS § 24A.140." 2009.

Murer, Amanda C. "Communication is the Key in Court Security in Report on Trends in the State Courts." p. 19. 2005.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=127>.

National Center for Judicial Security. *U.S. Marshals Service*.

<http://www.usmarshals.gov/oca/ncjs.htm>.

National Sheriffs' Association. *Court Officers and Deputies Association*.

<http://www.sheriffs.org/coda/index.asp>.

National Sheriff's Association. "Court Security Resource Guide." p. 18. 2008.

New York State Unified Court System. "The Task Force on Court Security Report to the Chief Judge and Chief Administrative Judge." 2005.

http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf.

New York State Unified Court System. "The Task Force on Court Security: Report to the Chief Judge and Chief Administrative Judge." p. 15. 2005.

http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf.

New York State Unified Court System. "The Task Force on Court Security: Report to the Chief Judge and Chief Administrative Judge." p. 41. 2005.

Pines, Zygmunt A. "Prudent Risk Management: A Court Administrator's View." *Justice System Journal*, Vol. 28, No. 1. 2007.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=85>.

"Protecting Judicial Officials: Implementing an Effective Threat Management Process." *Bureau of Justice Assistance Bulletin*. p. 4. 2006.

<http://www.ncjrs.gov/pdffiles1/bja/213930.pdf>.

Chapter 10: New Courthouse Design

Importance of Security Considerations in Designing a New Courthouse

Most courthouses in this country were designed and built at a time when concerns about security were not at the high levels that exist today. As a result, courthouse design poses significant constraints in terms of the security measures that can be effectively put in place. A prime example of this is, in most courthouses, in-custody defendants who are escorted to and from the courtroom through hallways in judges' chambers areas or through public space. This practice puts judges, court staff, and the public at potential risk. It is far better from a security standpoint to escort in-custody defendants only through "zones" or hallways dedicated exclusively for such use. However, the design of courthouses frequently makes this solution impossible.

The prospect of building a new courthouse presents a significant opportunity to build optimal security features into the very design of the building. Of course, security is only one of several major factors that need to be taken into account when designing a new courthouse. Aesthetics, accessibility, functionality, and technology are examples of other important considerations. However, events since 2000, including the 9/11 terrorist attacks, high-profile incidents of courthouse violence, and natural disasters, have resulted in an ever-greater emphasis on security in courthouse design and techniques for providing a safe and secure environment for staff and the public as well as the protection of records and physical assets.

Courthouse design guidelines routinely stress the multiple decisions that will be made in the course of planning, designing, and constructing a court building and the fine balance that must be maintained among various considerations. At a fundamental level, the design of each courthouse will reflect the basic decisions made on variables such as size, type of calendar, space for special programs, expansion needs, location, geography, and site context. Aesthetic, functional, and security requirements will have to be balanced with the short- and long-term costs of construction and operations. Security will have to be balanced with openness. Ensuring that courthouses are, and appear to be, open to the public and that they fit with their environment is a recurrent theme in the various court design guides and court facility standards that have been promulgated at the

federal and state levels. While security is only one of many elements to consider, it is clearly a critical one.

Incorporating Security into Design

Security, as a critical element of basic courthouse design, should be addressed at the beginning of the planning process and throughout the design process. The architectural/engineering team planning and designing the courthouse should consider the security implications of every aspect of design. Security equipment and personnel alone cannot do an effective job when constrained by courthouse design. It is clear that few agencies have sufficient resources or justification to implement every possible security countermeasure for every conceivable scenario; however, integrating security throughout the design process can provide an appropriate balance between security and other considerations.

The California Trial Court Facilities Standards (CTCFS) emphasize the importance of a comprehensive court facility security plan that integrates design, technology, and operations, including policies, procedures, and personnel, noting that “the most effective security plan is achieved when these three elements are coordinated during early project phases” (CTCFS, 2006: 4-3). The CTCFS define these elements as follows:

- **Design.** *Design* includes architectural elements and engineering systems, including space planning, adjacencies, user group zoning, passive physical protection, doors, locks, site perimeter barriers, exterior lighting, egress and circulation system, and all building systems relating to building evacuation.
- **Technology.** *Technology* includes electronic security systems and equipment, such as automated access controls, alarm monitoring, duress alarms, remote door and gate controls, closed-circuit television (CCTV), and cameras.
- **Operations.** *Operations* refer to policies and procedures for the court facility and those applied for security program management, security staffing, and employee training.

The importance of a comprehensive and balanced approach to courthouse security is also reflected in other materials developed in this handbook for the Ten Essential Elements for Effective Courtroom Safety and Security Planning, including Element 1: Standard Operating Procedures, and “Appendix A.” The approach should also be

collaborative and incorporate the perspectives of court personnel, space planners, architects, security experts, and, in the instance of site security, members of the community. All participants in the planning and design process should be educated about the fundamental objectives and concepts surrounding security in the court environment.

Design guidelines and standards for court buildings categorize and integrate recommended and mandated security measures in different ways. One of the more recent and comprehensive set of security guidelines is presented in the *U.S. Courts Design Guide* (published by the Judicial Conference of the United States Courts), which divides the discussion of courthouse security systems and equipment design into *exterior* and *interior* security. The specific guidelines on each topic are not reproduced here because (1) they are extensive; (2) they reflect requirements for federal courthouses that may or may not be applicable, cost-effective, or fit the context of the wide variety of state and local court building projects; and (3) they are readily available at the General Services Administration Web site. However, a review of the topics is useful to illustrate the broad range of considerations related to security that should be addressed in the planning and design phase even if the ultimate solution might not conform to federal specifications.

Exterior Security

According to the U.S. Courts Design Guide (USCDG) exterior security includes considerations of site, parking, lighting, access control at building entrances, and intrusion-detection/alarm systems. Specifically, the USCDG provides requirements for

- **Site** – building setback, landscaping, site lighting, separation of vehicle circulation, and closed-circuit television (CCTV)
- **Parking** – restricted and separate parking for judges, employees, and visitors monitored by CCTV cameras
- **Building Perimeter** – intrusion-detection system, windows, emergency exits, and CCTV cameras
- **Building Entrances** – public entrance, employees' entry, judges' entry, and the loading dock

In addition to the specific guidelines on site security contained in the USCDG, the General Services Administration's *Site Security Design Guide* provides an in-depth look at this issue, including the principles underlying the effort, the tools that are available to

designers, and a hypothetical test case where the principles and tools are applied. The authors acknowledge the complexity of site security issues and cite the following challenges for building designers: “determination of threats and vulnerabilities, which remain difficult to predict; decisions about what to protect, which may be fraught with emotion; and selection of countermeasures, which are often extremely expensive.”

The *Site Security Guide* advises that in order to balance aesthetic goals with security requirements, both the emotional and technical arguments about security must be considered, and the most acute needs must be addressed while being mindful of available resources. Successful site security design projects should adhere to four principles:

1. A strategic approach to reducing risk defines priorities; identifies correctable conditions; leverages resources to implement appropriate facility design, site design, and property management; and remains flexible to changing levels of threat.
2. A comprehensive design satisfies multifaceted site requirements to maximize functionality, aesthetics, and a total project value for its users and the community-at-large.
3. A collaborative, multidisciplinary team — including the court and tenant agencies, security professionals, designers, and community representatives — can integrate diverse expertise to create innovative and effective solutions.
4. A phased, incremental development strategy is invaluable for the successful implementation of security improvements over time, whether for a major project with multiyear execution or for multiple, small projects at one property.

The California Trial Court Facilities Standards also stress the importance of risk assessment and strategic approaches to site security design and recommend applying Crime Prevention through Environmental Design (CPTED) principles in site and building master plans in the early phases of architectural and landscape design. The standards cite three basic CPTED strategies:

- **Natural surveillance** — The placement of physical features, activities, and people in such a way as to maximize visibility, thus preventing the opportunity of crime (*e.g.*, proper placement of windows overlooking sidewalks and parking lots, using transparent vestibules at building entrances to divert persons to reception areas, etc.). This strategy can be

supplemented with the use of security and police patrols and the application of CCTV cameras.

- **Natural and constructed access control** — Natural access control focuses on limiting and providing guided access through use of properly located entrances, exits, fencing, landscaping, sidewalks and roadways, signage, and lighting. This guidance helps deter access to a crime target and creates a perception of risk to a perpetrator.
- **Territoriality** — The use of physical attributes that express ownership, such as fencing, pavement treatments, signage, and landscaping, promotes a perception that these areas are controlled. In an area that is physically designed to protect designated space, people are more likely to challenge intruders or report suspicious activity, and the design itself causes intruders to stand out.

In addition to the specific guidelines on building entrances discussed in the USCDG, the General Services Administration and the U.S. Marshals Service have jointly published a *Design Notebook for Federal Building Lobby Security*. These guidelines and recommendations generally address the placement of security screening stations within federal building lobbies, including courthouses, and security station prototypes. Noting the “visual chaos” created by some security screening stations that were quickly assembled in existing facilities in response to increased security demands, the authors stress the importance of creating “a good first impression to those entering the building – one that depicts an aura of professionalism, conscientiousness, and capability.” The design notebook discusses the overall context of the lobby and the role of the free zone – the interior space that lies between the exterior plaza and the secure portions of the interior – in providing a user-friendly, unrestricted environment for the public that can also serve functional needs such as access to information or forms. The coordinated design of the exterior plaza, free zone, and secure lobby is described as an opportunity to support the security requirements of the building, including allowing sufficient space for visitors to queue prior to screening and accommodating the people who will wait for elevators or seek information after screening. The design notebook also describes three versions of the security station prototype – box scheme, planes scheme, and line scheme – and provides an outline of the typical procedures at a security screening station. Sixteen case studies on the layout and positioning of security screening stations in

various federal buildings are presented to allow designers to see the application of the concepts in various contexts. The authors caution that many factors will effect design decisions made in this area, including assessment of risks and vulnerabilities.

Interior Security

Under the USCDG, interior security includes personnel security, security of property and documents, access control to interior spaces, personnel movement and circulation controls, security aspects of spatial arrangements, and the coordination and integration of security and fire and life safety requirements.

Physical separation of public, restricted, and secure circulation systems is an essential element of courthouse security design, and the integrity of each circulation system must be maintained for all functions within the court facility. The USCDG specifically cites the importance of (1) providing judges with a means to move from restricted parking to chambers, courtrooms, and other spaces through restricted corridors; (2) providing jurors with a means to move between floors on restricted-access elevators without crossing public spaces or secure prisoner corridors; and (3) providing a means for security personnel to move prisoners from the vehicle sally port into central holding facilities and to holding cells adjacent to trial courtrooms without passing or entering public or restricted spaces.

Life-safety protection systems and emergency egress requirements are prescribed by standards found in federal, local, and international building, fire, and electrical codes. The USCDG advises that a fire and life safety system should be equipped with an emergency evacuation system (EVAC) regardless of the number of occupants or floors. And recently it has been recommended that an automated external defibrillator (AED) be centrally located on each floor of court buildings.

When activated, intrusion detection systems, duress alarms, and other internal alarm systems in a courthouse should electronically report to a central command and control center.

The USCDG also contains guidelines on specific security measures for courtrooms, spaces associated with courtrooms, judges' chambers, jury facilities, libraries, clerks' offices, and court-related offices such as administration. These

guidelines outline what each of these spaces requires in terms of entry, type of windows, CCTV, security alarms, and other measures as appropriate to its function.

As a final thought in planning state courthouses, consideration should be given to designing additional security measures when warranted by specific kinds of cases. For example, domestic relations cases involving potentially volatile issues of divorce and custody have been statistically demonstrated to pose special security challenges. Courtrooms can be designed for such cases that include additional physical barriers and other means of providing extra security.

Bibliography and Resources

Hardenberg, D. and Phillips, T.S. (eds.). "Retrospective of Courthouse Design: 1991 – 2001." Williamsburg, VA: National Center for State Courts. 2001.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=76>.

Hardenbergh, D. *et al.* "The Courthouse: A Planning and Design Guide for Court Facilities." Williamsburg, VA: National Center for States Courts. 1998.

Judicial Conference of the United States Courts. "U.S. Courts Design Guide." Washington, DC. 5th ed. 2007.

<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=113>.

Judicial Council of California, Administrative Office of the Courts. "California Trial Court Facilities Standards." San Francisco, CA. 2006.

http://www.courtinfo.ca.gov/programs/occm/documents/06_April_Facilities_Standards-Final-Online.pdf.

U.S. General Services Administration (GSA). "The Site Security Design Guide." Washington, D.C.: Public Buildings Service, Office of the Chief Architect. 2007.

http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=23429

U.S. General Services Administration (GSA) and U.S. Marshals Service. "Design Notebook for Federal Building Lobby Security." Washington, DC. 2007

Utah Judicial System. "Master Plan for Capital Facilities." Salt Lake City, Utah: Administrative Office of the Courts. Vol. II. January 2008.

<http://www.utcourts.gov/admin/facilities/Section-II.htm>.

Appendix A:
Representative Sample of Guidelines
From
State Court Security Manuals

Standard Operating Procedures: Physical Security (perimeters, entryways, and interior areas)

A. Perimeter Security

1. Parking areas

- Parking should be secure, reserved, separated, and unidentified for judges, staff, jurors, and those subject to special security risks.
- Judges and staff should have direct access to secure corridors and elevators from the parking area. (See Michigan.)
- Vehicles should not have any features identifying the owner.
- Escorts or shuttles from the parking area to the facility should be available and provided on an as-needed basis for those with special security needs.
- Parking areas should be sufficiently illuminated and patrolled.

Security in these areas can be augmented by posting of emergency telephone numbers, placement of emergency phones, CCTV cameras, panic/call stations, assigned security personnel, entrance booths with guards, intrusion/detection devices, space assignments and design, passive/active physical barriers, card keys, and landscaping. (Wisconsin)

2. Grounds (lighting, visibility, protective distance)

- Perimeter areas should be adequately illuminated and properly landscaped to prevent concealment and in order to maximize visibility of persons and objects.
- Physical barriers (e.g., bollards, planters, fences) can be installed to provide at least a 50-foot set-back from the facility. For new structures, 100 feet is the recommended set-back. (See Wisconsin.)

3. Exterior of buildings (potential access routes)

- All potential openings or access points into the building (such as doors, windows, skylights, ducts, grates, etc.) should be secured to prevent entry or tampering, especially at the ground floor level.
- All access points should be properly illuminated.

4. Surveillance (patrols, daily inspections)

- Perimeter (including all grounds, parking areas, garages, common areas, doors, windows, potential openings) should be subject to routine inspection patrols on a 24/7 basis.
- All security problems encountered in such patrols should be promptly reported, documented in a report, and promptly addressed.

5. Equipment (alarms, surveillance)

- All entrances and portals should be equipped with intrusion alarms.
- Video surveillance (CCTV) for these areas is also recommended and, if employed, should be effectively monitored at all times.
- All security equipment should be regularly maintained and professionally tested pursuant to a schedule. (See New Jersey, Michigan, Washington, and Arizona.)

6. Loading docks

- Protocols should be developed for on-site deliveries (e.g., requiring identification of drivers, advance notice of deliveries, assigned personnel and equipment to screen deliveries and packages). (See Delaware.)

B. Entrance Security—Access to the Facility

1. Limited access (the “single point of entry” concept)

- Access points to the facility should be limited in number, preferably limited to one main entrance (the so-called "single point of entry").
The "single point of entry" is an important component of court security because, when used in conjunction with the screening post, it greatly minimizes risk at the front end.
- All points of entry should be secured with adequate personnel and equipment at all times.
Limited access to a facility greatly minimizes security risks, allows better observation and detection, and helps to reduce the costs of weapons screening throughout a facility.
- There should be continuous monitoring of all points of entry.

2. Controlled access ("the screening post")

- All persons entering the facility should be screened at all times.
Entrance screening is viewed as the single-most important element in a comprehensive courthouse security program. (For examples, see, Arizona, Ohio, Washington.) New Jersey exempts judges, and in New York, limited classes of persons – court employees, tenants of courthouse facilities, attorneys, government or non-profit agency employees who regularly conduct business within the courts – generally are not required to pass through magnetometers provided they comply with certain conditions (e.g., presentation of identification cards through the court's SecurPass program, which requires a criminal background check).
- There should be weapons screening at every access point.
Michigan's manual specifies that if staff and judges use non-public entrances, provisions should be made for weapons screening at such entrances. Entrances without screening should be locked and equipped with alarms and signage stating "Emergency Exit Only. Alarm Will Sound." Michigan specifies that a court's screening policy should include a list of restricted items, a secondary screening policy for people who have not successfully passed through after two tries, storage and disposal of confiscated items, protocols for appropriate responses to attempts to bring weapons in the facility, and protocols for law enforcement personnel. Michigan's manual also specifies the components of a proper weapons screening station to include adequate room for people to congregate inside, out of the weather, without being so crowded as to present additional security problems; a magnetometer, x-ray equipment, and handheld magnetometers for back-up screening; a duress alarm to summon additional help if needed; CCTV for monitoring access points; adequate staffing of at least two trained staff to monitor traffic flow and at least one officer with a weapon to observe and respond to emergencies; and access to a private area to conduct a more thorough search using same-gender personnel.

- If there is a separate entrance for judicial officers, the court's protocol should strictly prohibit admittance by any unauthorized persons.
- Items (such as purses, backpacks, briefcases, bags, boxes, laptops, CD players, cell phones, pagers, radios, etc.) should be subject to the screening process.
- Screening stations should consist of a metal detector, x-ray machine, and sufficient personnel to operate the equipment and conduct screening.
Ohio, for example, recommends at least one portable walk-through magnetometer and one handheld magnetometer with a trained security person. The preferred security practice is to have three personnel at each security screening post: one to operate the machine, one to check persons who set off a detecting device, and a third person who can provide back-up in the event of an emergency or need for additional screening procedure. (For example, see "Gaining Access to Courthouse Security," Courts Today, pp. 34-37, Jan-Feb 2005.)
- There should be clearly written, visible signage at the entrance indicating the court's screening policies and list of prohibited items.
Signage operates as a deterrent.

3. Screening of mail and deliveries

- All incoming mail and packages should be received in a central location and subjected to screening prior to delivery.
See Wisconsin's manual (Chapter 5) for an identification of characteristics of suspicious packages and appropriate response procedures. (Also, see Washington.)

4. Personnel (at entrance points)

- The complement and competency of trained security staff should be sufficient to operate court security equipment to control access to the facility. There should be pre-employment criminal background checks for all new personnel and a policy requiring employees to report promptly if they have been arrested or charged with a crime.

5. ID and access control procedures

- Identification procedures and protocols are helpful to reinforce entrance screening (such as card keys, identification badges, sign in/sign out, etc.). Such procedures should apply to all employees and visitors.
- Identification should be displayed at all times in the building.
- There should be strict control of all access keys and cards.
The use of badges and card keys must be strictly controlled and monitored, especially with regard to terminated or departing employees. A log of all such ID badges and cards should be maintained. Lost or stolen cards should be reported promptly. (See Arizona SJI Project regarding monitoring and auditing access cards, and Michigan and New Jersey. New Jersey provides for electric latch or card access entry for judges' private entrances.)
- Access codes should be periodically changed (especially after a security breach) and courts should have the ability to act promptly in the event of a security breach of its identification system.
New York, for example, utilizes a "smart card" system that physically incorporates digital chips that can be promptly deactivated. The New York security taskforce

recommended there should be sufficient information infrastructure capability to transmit data promptly to court administrators and the smart card system in order to deal quickly with misuse, forgery, or recall of such cards.

6. After-hours operations

- After-hours access to the facility should be limited and supervised.
- Security protocols (e.g., single access point, screening, and identification) should be employed on a 24/7 basis. (See New Jersey and Michigan.)
- There should be continuous monitoring of all access points.

7. Weapons policy

- Every facility should have a clear and strictly enforceable weapons policy, one that also addresses possession of weapons by law enforcement officers in the facility and courtrooms.

The New York security taskforce recommended that all firearms carried by uniformed on-duty personnel be secured in safe and serviceable holsters with a safety rating of Level III and that all court clerks authorized to carry firearms should be required to use holsters with covered trigger guards and snap enclosures that securely attach to their belts and to wear their uniform blazers at all times. Many states prohibit law enforcement officers (when acting outside the scope of their employment) from bringing weapons into a court facility. The carrying of weapons in a court facility is a difficult practical, political, and policy issue for many jurisdictions. Some states address the issue statutorily. In a 2005 survey conducted by the Delaware Administrative Office of the Courts, the overwhelming majority of responders indicated there was no formal court policy governing whether judges are permitted to carry guns in the court facility. Some states (e.g., South Carolina and Kentucky) apparently permit. Rhode Island and Allegheny and Berks counties in Pennsylvania reportedly have a zero tolerance weapons policy for court facilities. (Also see Michigan, Ohio, New Jersey [which exempts judges from weapons screening], and Alabama.)

- All personnel authorized to carry firearms in court facilities should be required to pass a qualified certification program successfully and be required to pass an annual firearms requalification program. (See Alabama.)
- There should be clear signage at the court's entrance regarding the facility's weapon policy.
- There should be secure depositories for the temporary storage of firearms.
- Unauthorized firearms and weapons should be confiscated and destroyed.
- Annual statistical reporting regarding seized weapons and contraband is advisable.

8. Other policy considerations: use of force and contraband

- Courts should have clear policies on use of force by court security personnel (when appropriate, acceptable physical responses).
- Courts should have clear policies regarding contraband items.
- Courts should have clearly stated and visible signage at court facility entrances and interiors about prohibited items subject to confiscation.

9. Custodial services

- Custodial staff should never have unsupervised access to the facility after hours.
- Custodial staff should be subject to routine security screening procedures.
- Custodial staff should be subject to initial and periodic security background checks.

Other security protocols should be considered, such as the wearing of name/company badges, fingerprinting, specific procedures for day and night shifts, sign-in/sign-out procedures, security checks of supplies, restrictions on packages/bags, and possession of alcoholic beverages/ non-prescription drugs in the building. (See Delaware.)

10. Vendors/independent contractors

- Protocols similar to those for custodial staff should also be identified and implemented for non-employee occupants/visitors, including vendors and independent contractors working in the facility. (See Delaware.)

C. Interior Security — Generally

1. Circulation zones

- It is recommended that a court facility's space be segregated or separated into three distinct "circulation zones" – separate zones for judges and staff, the public, and prisoners.
- Access to zones should be controlled. Access keys and cards by non-security personnel should be limited and supervised by security personnel.

Circulation zones are mandatory in New Jersey for new or renovated court facilities. If such circulation patterns or zoning areas are not feasible, other options (e.g., designating off-limits areas except for authorized personnel with I.D. cards, installation of locking devices and monitoring system) may be available. Designated off-limits areas could include HVAC/utility/computer equipment rooms or closets, chambers, elevators, work stations, unused court rooms, hallways, stairs etc. Delaware has designated security levels for areas and user groups. (Also see Arizona.)

- Where such circulation zoning is not possible, adequate procedures should be in place to protect staff and public from prisoners (e.g., by escorting prisoners with adequate security guards and using appropriate physical restraints).
- Non-authorized personnel and visitors should be restricted to public areas at all times.

2. Locking devices (utility and environmental controls)

- There should be strict control of access to all controls for the environment and utilities, which should be protected by tamper-resistant locking devices.
- There should be central administration to oversee the security of such controls.
- Outside air-intake mechanisms should be secured to prevent unauthorized access or interference. (See Michigan, Wisconsin, Arizona, and Delaware.)

3. Identification and monitoring procedures

- All personnel and authorized visitors should display appropriate identification at all times when in the facility.

Michigan specifies that an employee's identification card should display only the first name. New sophisticated technology is available to control and monitor access (e.g., electronic access cards or biometric systems that record a person's movement in the building). For examples see New York and Michigan.

4. Security equipment and enhancements

- Court facilities should be equipped with intrusion and duress alarms.
Intrusion alarms are designed to alert others to unauthorized entry after hours or in restricted areas. Duress or panic alarms are designed to signal to others (usually law enforcement or security officers) the need for immediate assistance at a specific location.
- Halls, corridors, and passageways should be brightly lit and equipped with viewing mirrors.
- There should be emergency back-up for lighting.
- Ceiling panels should be secured to prevent intrusion.
- First-aid kits should be readily available throughout the facility.
- There should be properly trained personnel to operate security equipment effectively.

In addition to x-ray machines and magnetometers to provide entrance security, devices to provide interior security include ballistic-shielded benches; caller ID phones; card-key readers; closed-circuit television cameras (CCTV); door viewers; electronic mechanisms to control opening and locking of doors; intercoms; locks to store and secure property (e.g., guns, cell phones, etc.); magnetic locks; numeric pin pads; restraining equipment (handguns, knee/ankle braces, Tasers); security lighting; and smoke detectors. Ohio recommends that, when practical, CCTV surveillance should include the court facility, parking areas, entrance(s) to court facility, courtrooms, and all other public areas of the facility.

5. Security personnel (training and safety)

- Security personnel in the facility should be adequately trained and certified in the skills and performance standards required to fulfill their responsibilities.

Such training should include instruction in the transportation and restraint of prisoners, facility-specific security procedures, the use of force, dealing with the public, etc. The New York court security taskforce recommends that each officer providing security to the facility should be given a copy of the facility's security protocols and acknowledge receipt thereof. (Also see New Jersey, Wisconsin [Chapter 9], Arizona [pp. 24-25], and Michigan. Arizona provides that "training of

court security personnel shall be career oriented with a core curriculum that is court security specific." New Jersey requires training in dealing with the public.

- The physical safety of security personnel to perform their responsibilities should be addressed.

The New York security taskforce recommended a court policy that requires court officers serving in sensitive posts and patrols to wear ballistic-resistant vests approved (and perhaps funded) by the judiciary and, further, that all such vests should be standard issue for all uniformed court officers. The New York report also recommended that some (but not all) security officers should be equipped with batons and O.C. (oleoresin capsicum) pepper spray in accordance with applicable laws.

6. Internal communications (within the facility)

- Each facility should have a public address system for use in the event of an emergency (such as lockdowns, bomb threats, etc.). Evacuation routes and emergency exits should be conspicuously identified.

7. Prisoner transport/holding areas

- There should be separate and secure holding areas where prisoners can be locked up and supervised (e.g., by security personnel, CCTV) while waiting to appear in court or to be returned to jail.
- Local corrections departments should notify the facility of any special category of prisoner (e.g., assaulting prisoner, escape risk, suicide watch, and gang affiliation) prior to transport to the court facility or, at the least, upon arrival at the court facility.

A prisoner classification system, worked out by local law enforcement and the courts, can be used to transmit critical data. For example, color-coded, high-security restraints have been successfully used to identify high-risk prisoners in their facilities quickly and easily. Also see New York security taskforce report regarding notification.

- Prisoners should have a separate circulation route away from court personnel and the public, and out of sight of jurors.

Ohio provides that if a separate circulation route for prisoners is not feasible, then appropriate restraints (handcuffs, leg braces) should be employed. See this section for information regarding restraining devices.

- Prisoners should be monitored by cameras or tracking devices.
- Restraint equipment should be used in appropriate situations and should be readily available in the facility in the event that a prisoner becomes unruly or creates a security risk. Prisoners escorted in the courthouse should be restrained with handcuffs.

For example, see Alabama and New York. Restraining devices include handcuffs, transport leg braces, ankle restraints, waist chains, transport/custody belts, and elastic belts equipped with stun devices. It is important to be cognizant of the dangers of prejudicing a juror who views a defendant in such restraints. The New York security taskforce recommended that a prisoner should be rear-handcuffed at all times except when appearing before a jury and during extended hearings. Holding cells could also be equipped with a small rectangular insert to provide secured access to a prisoner when handcuffs need to be removed.

- Appropriately trained and physically capable law enforcement personnel, in sufficient ratio to the perceived risk, should escort prisoners to and from the facility and courtrooms.
- There should be clear written protocols to cover the following prisoner transport issues: (1) the staffing levels required to escort prisoners, (2) the arming of security personnel, (3) physical requirements of escort personnel, (4) restraint/force procedures, (5) procedures to handle potentially volatile prisoners, and (6) emergency procedures in the event of an escape or evacuation.

For examples, see New Jersey, Delaware, Michigan, Washington, Ohio, and Arizona. Also see the publication by the National Sheriffs' Association ("Court Security Audits, Forms, Policies, and Self-Assessment Tools") especially with regard to holding facility guidelines. A recent publication from the National Association for Court Management recommends that security personnel not carry weapons when handling detainees and that a single officer never move more than one person at a time. See National Association for Court Management, Court Security Guide, p. 21 (2005). The New York taskforce on court security, supra, made the following recommendations regarding prisoner handling: (1) the prisoner escort court officer in control and in proximity to the prisoner should be unarmed (which is reportedly the current practice in New York City courts); (2) the number of uniformed officers transporting prisoners must be commensurate with the security risk presented vis-à-vis the number of prisoners being transported and the location's physical characteristics; (3) prisoners transported through public areas of a courthouse should be escorted by no fewer than two uniformed officers; and (4) courts should strictly prohibit the changing of clothes by prisoners at court facilities. Michigan's manual recommends the following standards for holding areas for temporary prisoners: holding areas should be constructed to lessen the possibility of self-inflicted injury; be inspected daily for contraband; include doors that allow for easy observation; include toilet facilities; be checked by staff every thirty minutes; have CCTV monitoring, if possible; and have a self-contained breathing apparatus.

- Videoconferencing should be considered as an alternative to prisoner transport. *Videoconferencing (e.g., of arraignments) entails less risk and expense. For examples, see Missouri Statutes sec. 561.031 and Pennsylvania Statutes 42 Pa. C.S., Section 8703. Videoconferencing speeds the process, minimizes risk and cost, and can be useful in a public health emergency. Such an option, however, must comport with constitutional and statutory requirements.*

8. Building/personnel profiles

- Courts should maintain confidential files regarding up-to-date personnel lists, essential personnel information (e.g., contact persons, medical needs), and the facility's floor plans and allocation of space.

This confidential information should be readily accessible in the event of an emergency or operational breakdown. Tennessee, for example, specifies that "medical and family data on each judge should be kept in the clerk's office including blood type, allergies or reactions to medication, and any other type of medical problems that should be known in case of an emergency, and the names, addresses, and telephone numbers of the next of kin."

9. Daily inspections/sweeps

- A security plan should include daily and weekly inspections of the interior as well as the exterior and adjacent areas.
- Any suspicious conditions or activities should be reported immediately and properly documented.

See Wisconsin (pp. 27-31), Delaware, and New Hampshire (providing a helpful identification of the scope of daily security checks, which is described as "the first line approach to achieving a secure court facility"). See Arizona regarding weapons screening and daily security checklists. See section on security incident reporting.

10. Personal security: threats and risks

- There should be procedures to notify law enforcement promptly about threats against judges and personnel. All threats should be promptly documented in a security incident form.
- In preparing a comprehensive security plan, each court, in collaboration with law enforcement, should have procedures providing for the security of judges and court personnel when needed at times other than normal working hours.
- All courts should have secure parking areas for judges, staff, jurors, and witnesses who have been threatened.

For examples, see Michigan, Ohio, Wisconsin, and New Jersey. New Jersey outlines procedures to protect members of the judiciary who receive threats. Wisconsin (pp. 79-90) identifies how to assess/rank a threat and provides information about threat assessment techniques/responses, and the U.S. Secret Service's identification of conditions that indicate a greater risk of violence. Also, see Fein and Vossekuil, "Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials," (U.S. Dept. of Justice, July 1998). See information on Element 5 (threat assessment).

- Courts should have the ability to obtain a prompt professional assessment of any reportable threat against their judges and personnel.

D. The Courtroom

- Allocation of security personnel in the courtroom should be flexible to address the risks posed in a particular proceeding, the type of case (*e.g.*, family, *pro se*, criminal), the stage of proceeding (*e.g.*, sentencing), and the extent of anticipated media coverage.

New Jersey's recommended standard is to establish a system of allocating security personnel based upon the type of trial and the nature and number of participants involved in the given proceeding – indicators that can be classified into increasing degrees of risk (low, moderate, high). Others recommend that there should be a uniformed officer in the courtroom during all proceedings. See Arkansas, SJI Court Emergency/Disaster Preparedness Planning Project, "Planning for Emergencies," supra at p. 11 (2005). Arizona notes that it is a recommended standard not to include in the security officer complement any officers assigned to escort in-custody participants or protected individuals.

- If the facility does not have adequate screening at its entrances, then each courtroom should be equipped with security devices (e.g., magnetometer, surveillance cameras, and duress alarms).
- The number of public entrances to a courtroom should be restricted.
- There should be a pre-determined, effective means of non-verbal communication between the court security officer and designated court personnel (e.g., clerk, presiding judge) that could be confidentially used in threatening or emergency circumstances.
- There should be restricted access to light and environmental controls located in the courtroom.
- There should be a safe, quick, and accessible evacuation/egress route (via automatic locking door with peephole) in close proximity to the judge's bench.
- Coverings (e.g., drapery, opaque glazing, and blinds) should be installed on courtroom doors and windows to prevent a line of sight into the courtroom.

If feasible, windows should enhance security in terms of composition. Shatterproof windows consist of two standard sheets of glass with transparent plastic that break into a rounded grain instead of jagged shards. Bullet-resistant glass involves thicker lamination; the thicker the glass, the more resistant to the type of bullet. Bullet-resistant glass is substantially more expensive.
- Courtrooms should be locked when not in use.
- All objects (e.g., furniture, flagpole, utensils) that could be used as items of assault in the courtroom should be secured or removed.

For example, see Wisconsin (p. 51), containing an identification of "common weapons of opportunity" and recommendations for their safe use, noting that even the simplest of everyday objects can be turned into lethal weapons.
- There should be sufficient distance between the judge's bench and others (litigants, attorneys, public). The judge's bench should contain bulletproof (fiberglass resistant glazing) material and be separated by a rail from the audience.
- There should be a clear policy regarding the possession of guns in the courtroom by law enforcement and judges.
- There should be a clear policy regarding the possession of cell phones in the courtroom.
- There should be clear protocols and designated responsibility for opening, locking, and daily inspecting of courtrooms.
- Clear protocols should be in place to secure and store exhibits, especially firearms and drugs.
- Courtrooms should have essential security equipment and enhancements.

Important security equipment for a courtroom include silent duress/panic alarms (e.g., at the judge's bench, clerk's desk, sheriff's station) activated by a hidden switch/button and wired for immediate communication to a central location; ballistic shielding for judge's bench to withstand penetration of "off the shelf" bullets from handguns, including a .357 magnum; portable radios and phones (including walkie-talkie); telephone; heat/smoke detectors; CCTV, if feasible, to alert and record a security incident; intrusion alarms; emergency backup lighting and electricity; and high-quality cylinder locks on doors with a locking/release button controllable by

judge or sheriff. (For example, see Wisconsin, Arizona, New Hampshire, Utah, Delaware, and Tennessee.)

- Court audiences should be seated at all times. Security and court personnel should be mindful of spectators attempting to change seats or move toward the bench, the parties, witnesses, or the jury. (See Alabama.)
- The number of prisoners in a courtroom at any one time should be minimized. The number of prisoners in a courtroom should be proportionate to the security provided. (See Alabama.)
- There should be clear protocols for dealing with disruptive people in the courtroom.
- In the event of a power failure where emergency power backup and ambient light are not available, there should be a continuously charging flashlight or other light source available at the judge's bench. (See Alabama.)

E. High-risk Proceedings and Populations

- As noted, it is recommended that courts establish a system of allocating security personnel based upon various factors, including the type of trial, number of participants, media coverage, and degree of risk presented.
Arizona notes that in assessing courtroom risk and consequent security response, a federal task force has identified the following factors as most useful in determining the need for security: whether the matter is civil, family, or criminal; the stage of the proceeding (e.g., pre-trial, trial, post-trial); the type of case; the subject matter of the case; the number of persons and/or identity of other participants during proceedings (e.g., witnesses, spectators); the identity of the parties to the proceedings; the extent of anticipated media coverage. Also, see Wisconsin (Chapter 4), which identifies risk levels based on the type of trial. Wisconsin notes the need for an "operational plan" that includes detailed information on protocols and procedures, specifies in advance individual and team assignments, and includes directives and essential documents, emergency response procedures, communications procedures, and command post.
- Pro se* and domestic litigation may require special risk assessment, security safeguards, and segregated spacing as well as clear advance communication and cooperation with law enforcement.
- Jurors should be afforded safe, secure, and separate space and should have ready access to court security officers.
- Jurors should be provided with clear, simple, written information about the court's basic security procedures as part of the juror orientation program. (See Wisconsin.)
- Special security procedures should be available for sequestered juries.
- Likewise, special security considerations should be given to victims, witnesses, and those who have received threats.
New Jersey identified some essential considerations in drawing up a security plan for a high-risk trial as well as special considerations for civil commitment hearings at state institutions. See pp. 32-39.

F. Administrative Offices

- Administrative offices are critical to a court's operations and, therefore, should be properly protected like any other space in the court facility.
- There should be special security protocols for the handling, storage, and transport of money and negotiable instruments.
Cash on-hand and its equivalent should be limited.
- Access to administrative offices should be controlled and monitored. Useful security measures include physical separation of staff from public (*e.g.*, by use of counters, half-walls, window shields); secure storage/locking of important files; daily inspections/sweeps of office space; controlled/supervised access by custodial or off-hours workers; locking of all doors and windows after hours; restricted access to areas housing computers, their servers, and related equipment; policy requiring the prompt reporting of suspicious packages, suspicious activity, and security breaches.
Wisconsin (Chapter 5) provides helpful detailed advice concerning how to enhance office security generally and respond to specific situations. Arizona recommends that, when practical, there should be CCTV surveillance for the clerk's office.
- Security personnel should be readily accessible to the court's administrative offices.

G. Judicial Chambers (Controlled Access)

- Access to the chambers and staff of a judge should be strictly controlled and monitored.
For example, see prior section on security of administrative offices. Controlled access to judicial offices can be achieved through various devices: monitors, electronic access cards, duress alarms (at desks or work stations of the secretary, receptionist, and judge), caller I.D. phones, and self-locking doors, and off-limit hallways and stairs. Ohio recommends an effective secondary screening process at the entrance to a judge's office; there should be a separate and safe work area not accessible to the public.
- All exits should be properly controlled with security devices (*e.g.*, locking devices, alarms) and monitored.
- All exits should be conspicuously identified.

Appendix B

Steps to Best Practices for Court Building Security



STEPS TO BEST PRACTICES FOR COURT BUILDING SECURITY

FEBRUARY 2010

**Timothy F. Fautsko
Steven V. Berson
James F. O’Neil
Kevin W. Sheehan**

**Daniel J. Hall, Vice President
Court Consulting Services
707 Seventeenth Street, Suite 2900
Denver, Colorado 80202-3429**



Entry Screening – A Court’s First Line of Defense

Acknowledgements

The development and publication of this report has been made possible by the support and hard work of many people. The National Center for State Courts (NCSC) wishes to acknowledge the four authors of this document, Timothy Fautsko, Principal Staff at the NCSC, and especially security consultants Steven Berson, James O’Neil, and Kevin Sheehan for their work in identifying the categories, topics, and steps to best practices in court security contained in this document. The NCSC also extends its appreciation to three practitioners in the field who carefully reviewed this document and made important recommendations that have improved the final product. They are Malcolm Franklin, Senior Manager, Emergency Response and Security from the Administrative Office of Courts in California; Frank Lalley, Judicial Security Administrator from the Administrative Office of Pennsylvania Courts; and Carol Price, Court Security Director from the Administrative Office of Courts in Utah. Their many years of experience in the field of court security and emergency preparedness proved invaluable in validating the many steps to best practice. Without their assistance, the quality and usefulness of information contained in this report would not have been possible. Finally, the NCSC extends thanks to its editorial staff – Ephanie Blair, Judy Amidon, and Lorie Gomez – for the many hours they spent providing quality assurance in the conformation and final editing of the report.

Introduction

The National Center for State Courts (NCSC), through its Court Consulting Division, has conducted security assessments of court buildings as well as personal security and safety training throughout the country. In conducting court building assessments, the NCSC assessment team has evaluated court security in terms of “best practices” – guidelines describing those security measures that should be in place with respect to a comprehensive set of topics covering court buildings and court operations. These best practices are not only based on the considerable experience of NCSC assessment team members, but are also a compilation of various guidelines from the U.S. Marshals Service, National Sheriffs’ Association, International Association of Chiefs of Police, the Transportation Safety Administration, the Department of Homeland Security, and the National Association for Court Management. The NCSC assessment team recommends that leadership in every court building strive to achieve best practices in all topic areas to provide a suitable level of security for all those who work in or visit the court building.

Acknowledging that implementing best practices in court building security will require increasingly scarce budgetary resources, the NCSC assessment team has also developed steps in phases that can be taken toward achieving best practices in various areas of court building security. These steps may be a useful approach to courts as they strive to implement improvements in court building security. The NCSC assessment team wishes to emphasize that a fully effective integrated level of security will be reached only when all the measures at the best practices level are incorporated. The NCSC assessment team has provided these steps in phases, so that a court at its discretion can adopt incremental improvements before reaching the level of best practices. These steps in phases are plateaus along an ascending path to improvement – improvement the NCSC assessment team recommends that courts achieve over time.

It is important to note that *Steps to Best Practices* focuses almost exclusively on security matters. With rare exception, issues of emergency preparedness, continuity of operations, and disaster recovery are not within the scope of this document.

Security is not a one-time achievement. It is a serious and continuous goal and requires constant vigilance. Further, it must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and they can never be eliminated. But with proper attention and care, they can be minimized. Paying close attention to the recommendations contained in *Steps to Best Practices* will help courts minimize the risks.

Steps to Best Practices is organized by steps, phases, topics, and categories. It will be helpful for the reader at the outset to have a working understanding of each of these terms:

- Steps: These are specific buildings blocks, specific actions that courts can take to improve security.
- Phases: These are logical groupings of steps forming a temporary plateau in terms of security measures in place.
- Topics: These are the subject areas into which steps in phases are organized.
- Categories: These are sets of topics. There are four categories listed in priority order. (*Note: Topics within each category are listed in alphabetical rather than priority order.*)
 - Category A. These are fundamental topics that must be addressed first in order to provide a base on which to place all of the others.
 - Category B: These are topics that are extremely important to address.
 - Category C: These are topics that are very important to address.
 - Category D: These are topics that are important to address.

CATEGORIES AND TOPICS

Topic #

Category A: Fundamental

One	Command and control center
Two	Policies and procedures
Three	Security committee

Category B: Extremely Important

One	Access of people into court building
Two	After-hours access to court building
Three	Chambers
Four	Courtrooms
Five	Court security officer (CSO) staffing levels
Six	Duress alarms
Seven	Threat and incident reporting
Eight	In-custody defendants
Nine	Training

Category C: Very Important

One	Closed-circuit television (CCTV)
Two	Emergency equipment and procedures
Three	Interior access during business hours (circulation zones)
Four	Intrusion alarms
Five	Jurors
Six	Parking (particularly for judges)
Seven	Public counters and offices

Category D: Important

One	Cash handling
Two	Exterior/interior patrols
Three	Perimeter issues
Four	Public lobbies, hallways, stairwells, and elevators
Five	Screening mail and packages

Category A: Fundamental

The three topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices*.

- **Command and control center.** Without such a center, the necessary and vital technological tools for court building security – closed circuit televisions (CCTV*), duress alarms, and intrusion alarms – cannot be utilized or monitored in an effective manner.
- **Policies and procedures.** Without these, there is no way to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices* to inform the process of developing a comprehensive and cohesive set of policies and procedures.
- **Security committee.** Without such a committee, meeting regularly and empowered to exercise rigorous oversight on all matters relating to security within the court building, it is difficult, if not impossible, to properly assess and address the myriad security challenges facing court leadership.

**CCTV, as used in this document, refers to a variety of old and new technologies. For detail, see topic C-1.*

TOPIC A-1: COMMAND AND CONTROL CENTER

Phase One

1. Establish a command and control center in the lobby area of the court building with an assigned court security officer (CSO*). For smaller court buildings, the monitoring function of a command and control center can take place at the front entrance screening station.
2. Provide for telephone/radio communication as a point of contact between a CSO and potentially vulnerable areas of the court building, such as courtrooms.

**Note: CSO is defined as an individual trained in court security and certified to use a firearm. The CSO should also be armed with a triple-retention holster and a radio that can communicate with the command and control center. The CSO at the command and control center does not necessarily need to be armed.*

Phase Two

Continue all steps in Phase One, plus add the following:

3. Design and construct a command and control center that is isolated from the main lobby of the court building.

4. Design a control panel that will provide space for administrative activity and equipment to monitor CCTV cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and radio dispatches.

Best Practice

Continue all steps in Phase One and Two, plus add the following:

5. Install control panels and monitoring equipment for CCTV surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch.
6. Provide additional security personnel as required to supervise and monitor command and control center activities.

TOPIC A-2: POLICIES AND PROCEDURES

Phase One

1. Judicial branch leadership understands the need for and commits to the implementation of effective, comprehensive security based on best practice models and establishes orders directing court security policies and procedures.

Phase Two

Continue with the step in Phase One, plus add the following:

2. Establish a task force under the direction of the court security committee (see Topic A-3) and with the cooperation of the appropriate law enforcement agency(s), to draft essential documents for the establishment of the policies and procedures on court building security. The task force on policies and procedures should include:
 - Court administration
 - Security personnel
 - Facilities management
 - Fire and rescue personnel
 - Others responsible for and impacted by court security
3. Create the package of essential documents to include:
 - Policies and procedures
 - Overall court security operations
 - Screening protocols
 - Define contraband that cannot be brought into the court building and confiscate it at the door.
 - Procedures to govern courtrooms and other areas in the event of a security incident
 - Risk and resource assessment instruments and protocols for use
 - Incident reporting instruments and protocols for use

- Operations manuals and materials
- Training manuals and materials
- Administrative orders with authority to revise

Phase Three

Continue all steps in Phases One and Two, plus add the following:

4. Establish communication to stakeholders that allows for feedback and adjustments as follows:
 - Assign a liaison between task force and stakeholders.
 - Provide periodic briefings in various formats to stakeholders.
 - Solicit formal feedback from stakeholders.
 - Adjust package (e.g., policies, procedures, manuals, materials) as necessary.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

5. Provide training and evaluate the package as follows:
 - Train everyone with a direct role in court security.
 - Conduct drills to test procedures.
 - Evaluate results of the drills.
 - Evaluate results of response to actual incidents.
 - Modify the package to improve practice.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

6. Review and update policies and procedures at least every other year.
7. Analyze Phases Two through Four for operational effectiveness.

TOPIC A-3: SECURITY COMMITTEE

Phase One

1. Establish a court security committee at the court building, which is chaired by a judge (preferably presiding) and has a membership of at least the primary security provider, such as the sheriff or CSO, the clerk of court, and the court administrator.
2. The judge or court administrator should meet regularly with law enforcement officials to discuss security concerns and improve security at the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Add the district attorney and public defender or representative from the state bar to the court security committee.
4. Add tenants to the security committee as appropriate.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Add elected officials to the court security committee.
6. Add an ad hoc member to the court security committee to serve on a task force for the committee.
7. Undertake a self-assessment of the security in place within the court building. Checklists with which to conduct these assessments are available from various sources, such as the National Sheriff's Association. Assistance in conducting assessments is also available from the NCSC.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Establish an integrated court security committee and use task forces to provide the committee with additional research and information gathering capacity. Additional members added to the committee or task forces should include:
 - Court staff members working in the court building
 - Local and state government officials
 - Local and state subject matter experts
9. Reconstitute the court security committee to be additionally responsible for emergency preparedness, disaster recovery/continuity of operations (COOP) plan, and response to pandemic flu, and add members with this expertise as appropriate. Rename the committee the court security and emergency preparedness committee.
10. Add planning responsibility for building new or improving current court facilities to the newly named committee.

Category B: Extremely Important

TOPIC B-1: ACCESS OF PEOPLE INTO COURT BUILDING

Phase One

1. Establish only one main door through which the public can enter the court building and display a sign at the entrance clearly listing those items that cannot be brought into the court building.
 - Designate one or more of the doors to the building to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through public entrances.
 - Keep all other exterior doors locked during business hours.
 - Emergency exit bars should be installed on all external exit doors. All exit doors should be alarmed, with ten second delay consistent with local codes. Establish signage that explains the “Exit Only” requirement.
 2. Establish protocols for entry through locked doors.
 - Tailgating* or bringing in family members/friends through these doors should not be allowed.
 - Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.
- *Note: In this context, tailgating is when an individual(s) enters a court building with a person who is authorized to properly gain entry with an access card or key.*
3. Assign one CSO to guard the public entrance to the court building on a full-time basis.
 4. Set up a table or other physical structure at the public entrance to serve as a screening station.
 5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
 - Provide screener with a weapons ID chart.
 - Provide screener with a list of contraband items.
 6. Train the CSO for all Phase One tasks described above.
 7. Provide basic court security orientation training for judges and staff.

Phase Two

Continue all steps in Phase One, plus add the following:

8. Add a magnetometer at the main door (public entrance) to the court building.

9. Conduct a daily calibration and inspection of magnetometer, preferably by an authorized and trained supervisor.
10. Train CSO(s) in all tasks added in Phase Two, plus provide additional security training for judges, staff, jurors, and others.
11. Replace keys to the court building with access cards for judges, authorized court staff, and other building tenants' staff.
12. Install a CCTV camera at the main door (public entrance) to the court building.
13. Assign a second CSO* to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
14. Establish a code notification procedure between law enforcement and the court so screeners are aware if a dangerous person is likely to enter the building.
15. Add a duress alarm at the screening station.
16. Establish a policy that law enforcement officers entering the building on personal business may not bring in a weapon.

**Note: Staffing level in Phase Two is one full-time CSO at the screening station, plus one additional CSO for high-volume times.*

Phase Three

Continue all steps in Phases One and Two, plus add the following:

17. Install an x-ray machine at the public entrance screening station.
18. The second CSO referenced in step 13 should be assigned as a full-time, permanent CSO* to operate the public screening station. During slow periods, this second CSO can still be available for additional duties as described in step 13.
19. Establish additional policies and procedures for Phase Three operations as follows:
 - Conduct an annual inspection and certification of x-ray machines.
 - Provide a detailed, step-by-step manual and training on screening procedures.
20. Train CSOs in all tasks and provide security orientation training for judges and staff.
21. Add a CCTV camera at the judge/staff entrance door.

**Note: Staffing level in Phase Three is two full-time CSOs at the screening station.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

22. Assign a third CSO* to operate the public screening station: one CSO to operate the magnetometer, one to operate the x-ray machine, and one to handle problems. During low traffic times, the third CSO can assume another assignment. Ideally,

- all three CSOs should be armed, but at least one should be armed. (Armed CSOs should use a triple-retention holster.)
23. If two or more public screening stations are in operation, assign a fourth CSO as a supervisor to oversee operations.
 24. Install a magnetometer, x-ray machine, duress alarm, and CCTV camera to the judge/staff entrance. Consider allowing jurors to use this entrance.
 25. Assign at least two CSOs to the judge/staff entrance if staff or jurors use this entrance and at peak hours during the day. Otherwise, assign at least one CSO.
 26. Establish a universal screening policy. Universal screening means everyone entering the building is screened.
 27. When everything is in place, establish a policy that only law enforcement officers with responsibility for court security inside the building may bring a weapon into the building. Other law enforcement officers should be required to check their weapons in a lock box at the screening station(s).

**Note: Staffing level in Best Practice is three full-time CSOs for each public screening station, plus one additional CSO to supervise multiple stations, and two CSOs assigned to judge/staff/juror entrance.*

TOPIC B-2: AFTER-HOURS ACCESS TO COURT BUILDING

Phase One

1. Permit access into all areas of the court building via key or electronic card access. Keys and cards should be issued and controlled pursuant to a comprehensive accountability system that has been approved by the court's security committee.
2. Conduct background checks prior to issuing a key or access card to any person.
3. Conduct background checks for cleaning crews and any vendors granted after-hours access to the building. Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court.
4. Monitor the activities of the public while in the building after hours.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Eliminate the use of keys and implement the use of an access card system. As necessary, issue keys to a limited number of people only for emergencies, building maintenance purposes, and building security responsibilities.
6. Create a single access point into the court building that is guarded by a CSO who checks IDs and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
7. Update background checks periodically (at least annually).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

8. Conduct a full screening requiring everyone to go through the magnetometer and x-ray station.

TOPIC B-3: CHAMBERS

Phase One

1. Install a duress alarm at the judge's desk and in the chamber's reception area.
2. Test duress alarms regularly – at least monthly.
3. Provide training to judges regarding personal security and safety in chambers.
4. Escort judges when leaving a chambers area for a courtroom if chambers hall is unsecured.
5. Keep existing chambers window coverings adjusted so activities cannot be observed from outside the court building.
6. Conduct daily sweeps of chambers in the morning and at the end of the day.
7. Keep entrance doors to chambers area locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Assign at least one CSO or transport deputy to be present whenever an in-custody defendant is escorted through chambers hallway.

Phase Two

Continue all steps in Phase One, plus add the following:

9. Install vertical blinds as interior window coverings in all chambers.
10. Install duress alarms in conference room(s).
11. Plan for and conduct drills regarding emergency situations in chambers area.
12. Escort judges when leaving secure chambers and courtroom area.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

13. Assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallway, with one to clear the path ahead. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
14. Install ballistic-resistant material in all accessible windows (e.g., ground level, first floor). The recommended ballistic-resistant material should meet UL Standard 752, Level IV, unless a lower level can be justified by an assessment of the risks based on such factors as adjacent structures and geographic features associated

with the location of chambers. This level may be reduced based on specific security assessments.

15. Request cleaning crews to clean chambers at the end of the day when court staff is present, rather than at night.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

16. Install CCTV cameras in chambers hallways that lead to the entrance to chambers areas.
17. If feasible given the existing structure of the court building, establish a secure path for judges to go from chambers to courtroom (no escorting of in-custody defendants). If feasible, establish a secure path to escort in-custody defendants from holding cells to the courtroom without going through chambers hallways.
18. Install ballistic-resistant material in all chambers windows that are located on floors above ground level.
19. Prohibit cleaning crews from entering chambers unsupervised at any time. Require cleaning during the day or leave waste baskets outside locked chambers area doors at night. The judge or court staff should be present when cleaning crews are physically cleaning/dusting chambers during the day.

TOPIC B-4: COURTROOMS

Phase One

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a “rover” from one courtroom to the next (unless local or state rules require additional coverage). There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.
2. Install duress alarms in the courtroom at accessible locations:
 - On top of or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk’s stationTrain judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high-visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)

5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.
6. Install and then regularly test emergency lighting/fire equipment in courtrooms.
7. Always keep front and back doors to courtrooms locked when courtroom is not in use.
8. Use proper and acceptable restraints per state law on in-custody defendants.
9. Prohibit use of camera/cell phones in the courtroom and prohibit other items that could be used as weapons.

Phase Two

Continue all steps in Phase One, plus add the following:

10. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in the courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present.
11. Install one CCTV camera in criminal and family courtrooms.
 - The camera should be installed in the back of the courtroom in order to monitor activities in the courtroom up to and including the well and bench area.
12. Holding cells in the courtroom should be properly constructed and escape-proof.
13. Every three or four months, debrief incidents that have occurred in the courtrooms and review procedures related to courtroom security. This debriefing should take place in the courtroom. There should be an immediate debriefing on any serious security incident.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

14. A second CSO should be assigned to a courtroom whenever any court proceeding is being held. Whether or not there is an in-custody defendant, one CSO should be assigned for the judge and one for the courtroom. A second CSO is not ordinarily needed for civil cases, unless specifically requested by a judge based on a determination of a higher risk involved in a particular case.
15. Install one CCTV camera in all remaining courtrooms.
 - The camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
16. Install two CCTV cameras in criminal and family courtrooms.
 - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.
17. Begin the process necessary to establish a courtroom in the jail for advisements/arraignments and other hearings. Use video arraignment* originating

from the jail for in-custody hearings as much as permitted by state law.

**Note: Video arraignment is the preferred solution to bringing in-custody defendants back and forth for settings and brief hearings.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

18. For high-visibility trials, an additional CSO should be assigned to be present in the courtroom.
19. Use video or a courtroom in the detention center for all arraignments or hearings to set dates of next appearance.*

**Note: Use of video is the preferred solution to personal appearance by in-custody defendants whenever legally feasible by state law.*

20. Conduct sweeps of all courtrooms, including the random use of trained dogs.
21. Provide separate working offices (not in the courtroom) for clerks and others to use after courtroom proceedings have been completed.
22. Use bullet-resistant materials when constructing or retrofitting the bench and workstations inside the courtroom. The most recent recommended standard for these materials is UL Standard 752 Level III.
23. Install two CCTV cameras in all courtrooms.
 - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.

TOPIC B-5: COURT SECURITY OFFICER (CSO) STAFFING LEVELS

Phase One

1. One CSO* should be permanently assigned to the main entrance of the court building during business hours.
2. One CSO or transport deputy should be assigned to the courtroom while there is an in-custody defendant in the courtroom.
3. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a rover from one courtroom to the next. There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.

**Note: It is estimated that each CSO post requires approximately 1.33 full-time employees to cover for sick leave and annual vacation, training, etc.*

Phase Two

Continue all steps in Phase One, plus add the following:

4. As additional CSOs become available, assign in the following priority per recommended phases leading up to Best Practices in each relevant topic:
 - To meet recommended staffing guidelines at screening station (see Topic B-1)
 - To meet recommended staffing guidelines for the courtroom (see Topic B-4)
 - To meet recommended ratios for transporting in-custody defendants (see Topic B-8)
 - To assign patrols for the interior and exterior of the building (see Topic D-2)

Best Practice

Continue all steps in Phases One and Two, plus add the following:

5. Achieve full recommended staffing guidelines for the following topics:
 - Screening stations (see Topic B-1)
 - Courtrooms (see Topic B-4)
 - Transporting in-custody defendants (see Topic B-8)
 - Regular patrols of building interior and exterior (see Topic D-2)

TOPIC B-6: DURESS ALARMS

Phase One

1. Install duress alarms in the courtroom and at the bench, clerk's station, and CSO station. Training should be provided on the functionality of duress alarms and on the protocols for use.

Phase Two

Continue step in Phase One, plus add the following:

2. Install alarms in each chamber and reception area.
3. Install alarms at public counters, cash areas, and other offices where the public has access, including those without counters.
4. Install alarms in the interview and mediation rooms.
5. Install alarms and 911 contact ability at the childcare center, if the court building includes such a center.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. Install alarms at screening stations.
7. Install an alarm in the jury assembly room.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install duress alarms in the holding cell area.
9. Install a duress alarm in the loading dock area.
10. Install a duress alarm in the mailroom.

TOPIC B-7: THREAT AND INCIDENT REPORTING

Phase One

1. Establish a policy requiring incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible. The more serious the incident, the more quickly it should be reported.
2. Train CSOs and staff in the court building on how to define what an incident is and how to report incidents verbally and in writing.
3. Develop and use an incident reporting form and submit forms in writing to the proper authorities, at least on a monthly basis.

Best Practice

Continue all steps in Phase One, plus add the following:

4. Implement a practice for periodically evaluating incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court security committee (and the committee's incident reporting task force).
5. Provide general feedback to staff on incidents, particularly to those who reported them (e.g., complete the feedback loop).

TOPIC B-8: IN-CUSTODY DEFENDANTS

Phase One

1. Assign at least one CSO or transport deputy to escort in-custody defendant(s) through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO or transport deputy to remain with defendant(s) in the courtroom at all times.

3. Efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum.
4. When transporting in-custody defendant(s) in public hallways, bystanders should be moved to one side of the hall. When transporting in-custody defendant(s) in a public elevator, the elevator should be cleared of all other people.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
6. Make sure all holding cells and areas within the court building are appropriately structured, secured, staffed, and searched daily.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Install CCTV cameras along entire in-custody defendants' escort route.
8. Establish a secure sally port for in-custody defendants entering the building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

9. Establish a secure pathway for a defendant from the transport bus, through the sally port, to the holding cell and the courtroom to avoid crossing the path of judges, staff, or public.

TOPIC B-9: TRAINING

Phase One

1. CSOs should be trained in court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, and safety and weapons certification.
2. New judges and court staff should receive an initial court security orientation briefing that includes emergency procedures, building evacuation routes, building emergency color code system, and personal safety procedures for work and home.
3. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

4. All CSOs should receive at least 16 hours of mandatory in-service training on court security each year.
5. Establish a judge and staff security education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and at home.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. In addition to annual qualification with firearms, establish mandatory refresher court security training programs for CSOs, to include such topics as emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage, shooter-in-place, and judicial protection.
7. Establish mandatory, ongoing security and safety education programs for judges and court staff that include such topics as handling difficult people, home safety techniques, safety practices for inside and outside the court building, hostage incidents, and emergency evacuation from the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. In addition to annual qualification with firearms, establish annual mandatory refresher court security training programs for CSOs to include first-aid, defensive tactics, handcuffing, courtroom security, and judicial protection.
9. Establish mandatory ongoing security and safety education programs for judges and court staff that include handling difficult people, high-profile trials, home safety techniques, safety practices inside and outside the court building, hostage incidents, travel safety tips, threats, and emergency evacuation from the court building.
10. Train judges and court staff in self-defense and techniques for hostage-taking situations.

Category C: Very Important

TOPIC C-1: Closed Circuit Television (CCTV)

Phase One

1. Install a digital and color CCTV camera system* at the entry screening station and in the courtroom(s) facing the gallery.

**Note: CCTV systems can utilize various kinds of technology to transmit video images and to provide for system access and control. Cables have been the traditional means of system connectivity. Newer technologies have emerged over time. Some systems now utilize an internet protocol (IP) to transmit data and control signals over a fast Ethernet link. Another technology, virtual local area network (VLAN), allows authorized personnel to access cameras or a recorder from a remote setting. Courts are encouraged to explore and adopt the technologies that best suit their needs and budgets.*

CCTV cameras should have the following functional capacity:

- Fixed or pan, tilt, zoom. These types of CCTV cameras are typically used by most courts. Fixed cameras with a wide-angle lens allow for a stationary focus on areas of interest. The capacity to tilt and pan allows each camera to maximize its area of coverage, thereby minimizing blind spots and the number of cameras needed. The ability to zoom allows each camera to capture a more accurate and close-up picture of what is actually transpiring in a particular scene.
- Color. This is standard in current systems. Black-and-white images cannot tell the full story. Important features are indistinguishable. Only with a color monitor can faces and other specific objects be clearly identified.
- Recording capacity. The CCTV system should have digital video recording capacity enabling a CSO to view incidences at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation issues. The operation and recording function of a camera can be set to activate by either motion or sound, or by the setting off of duress or intrusion alarms.
- Signs. Notices should be conspicuously placed to inform the public that CCTV cameras are operating and recording activity in the area.

Phase Two

Continue the step in Phase One, plus add the following:

2. Install CCTV cameras in detention areas to monitor activities in holding cells.
3. Install CCTV cameras on building perimeters and in secure parking lots.

4. Install CCTV cameras to monitor activity at public counters and in offices where the public may visit.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Install CCTV cameras at the loading dock.
6. Install CCTV cameras in hallways.
7. Install CCTV cameras in each courtroom.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install CCTV cameras in elevators and stairwells.
9. Install CCTV cameras at screening stations.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

10. Install CCTV cameras in hallways that access chambers.
11. Install CCTV cameras in the mailroom.
12. Install CCTV cameras in the childcare area, if such an area exists.
13. Install CCTV cameras to cover all pathways through which an in-custody defendant may be escorted.
14. Install CCTV cameras to cover the interior areas of all doors to the court building and all accessible windows.

TOPIC: C-2 EMERGENCY EQUIPMENT AND PROCEDURES

Phase One

1. Use emergency color codes to designate emergency procedures for evacuation. An example of such a code system is attached as part of the Appendix.
2. Have an emergency, battery-generated lighting system in courtrooms, offices, and public areas.
3. Have a fire extinguisher on each floor, with egress floor plans posted.
4. Have fire alarms placed on each floor.
5. Have an elevator(s) that meets state and local fire codes, i.e., the national fire code that was developed after the MGM Grand Hotel, Las Vegas, Nevada fire, November 21, 1980.

Phase Two

Continue all steps in Phase One, plus add the following:

6. Have an emergency generator system that is properly fenced-in and protected.
7. Test generator system monthly; keep a log of tests.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Have CCTV cameras installed in the elevator(s).
9. Have automated external defibrillators (AEDs) located accessibly on each floor and designate a person(s) in the court building who is trained to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
10. Designate a floor warden on each floor to ensure proper response to emergency codes.
11. Have an enunciator fire alarm and extinguisher system.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

12. Have a floor warden identified and trained on each floor to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
13. Designate a safe area for a command and control center during an emergency.
14. Consider advising judges and staff by public address system, bull horn, email, or phone. One method of warning is the use of Court Building Warning Codes; a sample can be found in the Appendix.
15. Have an evacuation plan that everyone in the court building has been familiarized with.
16. Have a bomb-threat protocol and a lockdown plan in place.

TOPIC C-3: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES)

Phase One

1. Establish the concept of circulation zones (separate areas and routes) for the following:
 - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, back of public counters, private elevators, secure stairways)
 - In-custody defendant transport (e.g., routes for entering and exiting the

- building, to and from holding areas/courtrooms)
- Public (e.g., restrict the public to public zones)
2. All doors that are required to be locked, in accordance with the court buildings circulation zone concept, should be kept locked at all times. Such doors should never be left propped open.
 3. Have a key or access card system to control access based on a system approved by the administrative authority of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience. This system should
 - Be under the control of a central authority
 - Require background checks for all card or key holders
 - Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination)

Phase Two

Continue all steps in Phase One, plus add the following:

4. Eliminate keys and require access cards. Maintenance staff and emergency responders should retain keys.
5. Establish viewing ports (peepholes) to help prevent non-authorized access through secured courtroom doors.
6. Improve definition and enforcement of circulation zones.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Establish some form of video recognition (phone) system to allow access into secure areas.
8. Continue to improve definition and enforcement of circulation zones.
9. Install a CCTV camera system in all secure areas in the court building to monitor activity.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Establish and maintain maximum separation among zones (e.g., in-custody defendants are not escorted through secure hallways; judges do not pass through public areas when going to and from their cars, through screening, and to and from chamber areas.)

TOPIC C-4: INTRUSION ALARMS

Phase One

1. All exterior doors should have basic intrusion alarm devices, covering
 - All locked doors after hours
 - Emergency exit doors during business hours

Phase Two

Continue the step in Phase One, plus add the following:

2. Install intrusion devices on all accessible windows, either glass-break or motion detector.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

3. Establish a fully integrated intrusion system with the following functionalities:
 - When a court building is closed, every external door should be equipped with a device that will trigger an alarm at the control center of the appropriate responding agency and identify the intruded area.
 - During business hours, every door that is kept locked should be equipped with a device that will trigger an alarm that will identify the area intruded at the command and control center within the building. Every locked door with an emergency exit bar should trigger an alarm whenever anyone uses it, with a ten-second delay consistent with local codes
 - When the building is closed, this alarm should go to the control center of the appropriate responding law enforcement agency; when the building is open, the alarm should go to the building's command and control center.
 - All windows that are reasonably accessible from the exterior perimeter of the building (e.g., first floor, basement, possibly second floor) should be protected against intrusion. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

4. Integrate CCTV cameras into the system described above so that cameras will be activated in the area(s) of intrusion.

TOPIC C-5: JURORS

Phase One

1. Provide jurors with court security information before they report for duty by placing information on the jury summons they receive. For example:
 - Where to enter the court building
 - What items (e.g., knives, nail files, scissors) should not be brought into the court building
 - Not to discuss cases with anyone before and during jury service
 - Not to wear juror ID badges outside the court building
2. Screen jurors as they enter the court building or before they report to the jury assembly area.
3. Give a basic security and building evacuation orientation and ID badge to jurors at the assembly area before going to the courtroom. Cover such matters as what to do in case of an emergency and how to respond to a coded emergency announcement.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Assign a CSO to the jury room whenever juror payment is being made and when juror funds are obtained and transported back and forth to the court building.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

5. Assign a CSO to provide security inside and outside the jury assembly room when jurors are present.
6. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervise the loading of jurors and another CSO should meet the jurors on the floor on which they disembark.
7. Assign a CSO to remain with the jury during the entire trial/deliberation.

TOPIC C-6: PARKING (PARTICULARLY FOR JUDGES)

Phase One

1. Remove all signs in judges' parking area that identify spots either by name or title of judge. Any signs should simply say reserved along with a number as appropriate.
2. Each judge should notify law enforcement officials or a CSO of their arrival in the morning and be escorted into the court building if they park in an unprotected public parking lot.
3. Judges should be escorted to the unprotected parking lot by a CSO when they leave at night.

Phase Two

Continue the steps in Phase One, plus add the following:

4. Fence in the judges' parking lot and require that an electronic card access system is used for entrance into the court building. Install privacy slats if a chain-link fence is used.
5. Judges and court staff should be escorted to their cars or other mode of transportation after business hours.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

6. Provide secure parking for judges, court staff, and jurors.
7. Install CCTV cameras in secure parking lots.
8. Provide judges and court staff a regular patrol presence in the parking areas in the morning, during the lunch hour, and at close of business.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

9. Provide a secure parking area, preferably covered, for judges where they can proceed directly from their car, through screening, to their chambers without traversing any public areas or main court building entrance areas.

TOPIC C-7: PUBLIC COUNTERS AND OFFICES

Phase One

1. Install one or more duress alarms at the main public counter. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in offices (e.g., drapes, blinds) lowered to restrict observation from outside.
3. Install Plexiglas-type enclosures at cash counters.
4. Keep cash and checks in a secure, locked area overnight.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Install Plexiglas-type enclosures at all public counters.
6. Install duress alarms strategically in the back areas of offices.
7. Keep cash and checks and daily change locked in a safe overnight.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Install CCTV cameras at all public counters.
9. Install an alarm on the safe.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Install CCTV cameras overlooking the safe.
11. Provide regular security patrols by CSOs at the public counters.

Category D: Important

TOPIC D-1: CASH HANDLING

Phase One

1. Develop and train court staff on procedures for handling cash. The procedures should:
 - Determine who should collect the money
 - Determine how to safeguard money during the daytime work hours and overnight
 - Train staff on how to verify checks and reconcile fees
 - Determine industry standards for deposits
2. Install protective barriers and duress alarms at cash counters.
3. Use an office safe for money storage.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Install CCTV cameras at counters and in the office.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Use an armored car service or the bank's personnel to pick up funds daily.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require two people – one court staff and an armed CSO – when carrying cash.

TOPIC D-2: EXTERIOR/INTERIOR PATROLS

Phase One

1. Request that the local law enforcement agency conduct exterior patrols, particularly during times when the building is closed.
2. Develop a memorandum of understanding (MOU) with local law enforcement regarding which agency is responsible to protect the exterior of the court building during and after business hours.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Conduct regular CSO interior patrols by CSOs assigned to work in the court building, focusing on crowded hallways.
4. Assign CSO exterior patrols both regularly and randomly throughout the day.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Continue to increase both interior and exterior CSO patrols of the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require scheduled patrols of all interior and exterior areas 24/7, either by CSOs or local law enforcement officers.

TOPIC D-3: PERIMETER ISSUES

Phase One

1. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness. It should also be sufficient for perimeter CCTV cameras to capture images.
2. Keep doors locked after hours and allow access only via appropriately authorized key or access cards.
3. Keep all shrubbery and trees properly trimmed to prevent hiding places or access to the court building roof for persons or packages.
4. Conduct daily security checks around the perimeter.

Phase Two

Continue steps in Phase One, plus add the following:

5. Provide a secure parking area for judges with signs that do not indicate that the space is being used by a judge (e.g., signs should not say for official use only).
6. Install intrusion alarms to cover all exterior doors and accessible windows.

Phase Three

Continue steps in Phases One and Two, plus add the following:

7. Install CCTV cameras around the perimeter (at each corner of the court building).
8. Install bollards as necessary outside selected (main) entrance doors, ground floor (accessible) windows, and other vulnerable areas.
9. Enclose and secure all exposed utilities.

Best Practice

Continue steps in Phases One, Two, and Three, plus add the following:

10. Replace keys with an electronic card access system (except for back-up emergency) on exterior door entrances to the court building.
11. Provide secure parking for staff and jurors. Secure parking for judges and staff should have the following attributes:
 - Protected from public access
 - Protected from public view
 - Required electronic access, by way of card or other appropriate device
 - CCTV cameras in place and operating

TOPIC D-4: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

Phase One

1. Provide emergency lighting in the court building.
2. Establish egress/ingress standards regarding stairwells, hallways, and elevators.
3. Establish emergency procedure and evacuation diagrams.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Designate secure and public elevators.
 - Provide secure elevator(s) for judges.
 - Provide secure elevator for prisoner transport.
5. Install appropriate signage to alert the public to what items cannot be brought into the court building (i.e., guns, knives, scissors).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Install CCTV cameras in lobbies, hallways, stairwells, and elevators in the court building and provide secure elevator(s) with electronic card access.
7. Assign a CSO to regularly patrol these areas in accordance with an assigned schedule.
8. Install a public address system in the building to facilitate announcements and emergency codes.

TOPIC D-5: SCREENING MAIL AND PACKAGES

Phase One

1. Provide routine visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items.
2. Require staff to attend training on postal security and package identification techniques provided by the United States Postal Service (USPS).
3. Develop and practice a response protocol with law enforcement when a package is identified as suspicious or dangerous.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Require all mail and packages to be processed through an x-ray machine.
5. Require everyone delivering mail or packages to pass through the magnetometer.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Best practice is to establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:
 - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious) upon being received at the mailroom. This includes USPS mail delivered/picked up by court staff from the local post office.

- Deliveries of flowers, candy, food, gifts, etc., to any person located in a court building should be cleared through the mailroom first, be verified and vouched for by the recipient, screened as appropriate, and then delivered.
- Mailroom staff should sort incoming mail and packages off site by building, division, and/or department and prepare them for acceptance by designated representatives of each court office or division.
- Designated representatives of each court office or division should go to the mailroom, pick up mail for distribution to their offices, and identify questionable items. All authorized court and other staff mail handlers should attend training on handling suspicious mail. Local USPS or postal inspectors may conduct advanced training for state and local government agencies.

Sample Court Building Color Codes

Professional emergency responders advise that, as much as possible, communication during an emergency should be clear, understandable, and simple. Presently, state and local courts use different warning systems and language to advise court building occupants what to do during an emergency. The decision whether to stay or leave a court building during an emergency often can be the difference between life and death.

Realizing that clear communication and understandable instructions are vital, courts have been advised by the NCSC to use universal color codes and practice drills to augment their existing evacuation procedures. Using the same color-coded language in every court building will ensure that employees will understand and react properly to emergencies.

- **Code Yellow – Situational Awareness**
 - Cautionary: Be aware and prepared to react to danger.
 - A dangerous situation may be developing in the court building.

- **Code Red – Imminent Danger**
 - Stay put! An active shooter is in the court building or there is a hostage situation.
 - Get into an emergency protective posture or in a safe haven.

- **Code Green – Emergency – Evacuate Building**
 - Listen to instructions from your floor warden.
 - Report to your assigned location away from court building.

- **Code Blue – Emergency Team Responding**
 - An emergency team is responding to or is in the court building.
 - Wait for further instructions from officials.

- **Code White – Administrative/Informational**
 - Return to normal operations.
 - All is well.

Appendix C

Home Security Audit and Recommendations

National Center for State Courts

HOME SECURITY AUDIT AND RECOMMENDATIONS

Even though reports indicate that judges and other judicial branch personnel are more likely to be injured in a fall at home or in an automobile accident than in a work-related assault, increased violence in recent years has resulted in three judges being murdered at home. These deaths were directly connected to cases over which they presided. The home security audit that follows is designed to identify security risks and provide judges and other judicial branch personnel with basic personal security recommendations that can be used to protect them and their homes.

PERIMETERS/EXTERIOR OF THE HOME

1. Does the home have perimeter lighting? Yes No

Recommendation: It is important that the entire yard is illuminated at night, without shadows.

Recommendation: Install motion detector lights for interior and exterior protection. Outside motion detector lights can be installed to automatically turn on interior lights, giving the impression someone has entered a room, at the same time the outside lights turn on.

2. Does the home have trees and shrubs that are overgrown to the point where they block easy view from within? Yes No

Recommendation: Trim or remove thick shrubbery from window areas and replace them with shrubs that have thorns, like roses, near windows.

Recommendation: Trim or remove trees that may provide access to upper floor windows or balconies, and make sure trees or shrubs do not block a clear view of entries and windows from the street.

3. Does the home have outbuildings (detached garage, pool house, storage buildings) located on the property? Yes No

Recommendation: Include all outbuildings into the main security system. Install quality residential locks on the buildings.

4. Do all perimeter doors provide protection from intruders? Yes No

Recommendation: All perimeter doors should be solid core wood or steel with a deadbolt lock, in addition to any other locking device.

The door should have a peep hole installed to view any visitors prior to granting access to the home. No glass should be on the door that can be broken to gain entry. It is important that a three-inch strike plate for screws be installed in all entry doors.

Recommendation: Secure sliding glass doors with pins to prevent both horizontal and vertical movement, especially when the home is left vacant for an extended period of time. Sliding glass doors should be hung so that the sliding door is mounted on the inside. The door should be reinforced with a “jimmy-proof” bar to prevent forced entry.

Recommendation: Re-key or replace locks if keys are lost or stolen or if you move into a previously occupied residence. Make sure that you follow strict key control with keys used to access the home.

Recommendation: Be sure to restrict the number of keys to your residence. Keep keys in your possession. Do not hide keys outside under the mat, over doors, in mail slots, or in potted plants.

5. Are basement windows to the home secured? Yes No

Recommendation: All basement windows should be secured from inside the home. Glass basement windows should be replaced by polycarbonate material or reinforced with decorative security bars. All ground shrubs in proximity to the basement windows should be trimmed or removed so that they do not provide potential intruders with cover from observation.

6. Does the home have an attached garage? Yes No

Recommendation: Whenever possible, park vehicles in the garage. Always enter the vehicle from inside the garage. Always keep the garage doors closed and locked when not in use. In order to limit your exposure outside the vehicle during the hours of darkness, install an automatic garage door opener and make sure all family members know how to operate the garage door

manually in the event of an emergency. Ensure that the door from the garage into the main house itself is a solid core door with a deadbolt locking device.

Recommendation: If there is a vehicle parked outside, make sure the area is well-lighted. If at all possible, have a remote starter installed in all vehicles, especially if they are parked outside. This device will allow you to start your vehicle from a safe distance.

7. Does the mail box or the entry of the home personally identify the occupants? Yes No

Recommendation: Remove any identifying information from the mail box or entry of the home.

INTERIOR OF THE HOME

1. Does the home have an anti-intrusion alarm system? Yes No

Recommendation: Consider installing an anti-intrusion alarm system in the home that is tied into the local police department or a certified central alarm monitoring organization. Instruct family members on the operation of the system. Consider installing a local enunciation system or siren. The advantage of a siren is to alert neighbors to notify authorities, should the direct-connect alarm lines be compromised.

Recommendation: As an added security measure, alarm systems can be customized to provide monitoring for fire, medical alert, and closed circuit television (CCTV) surveillance of home exterior. The presence of cameras on the outside of the home is a definite deterrent to would-be intruders.

Recommendation: If you have a monitored intrusion detection system, display the monitoring company's decal or sign prominently on doors, windows, and in the yard to announce the presence of a security alarm system in the home.

2. Do you have smoke/heat detectors installed throughout the home? Yes No

Recommendation: Smoke alarms and heat detectors should be installed throughout the home. They should be hard-wired into the home's electrical system with a battery backup in the event

of a power failure. In addition, install and maintain all-purpose fire extinguishers throughout the home, especially in the kitchen.

Recommendation: Establish and periodically test fire evacuation procedures for all family members.

3. Is the exterior door leading from the basement to the upper floor made of solid core and equipped with a deadbolt lock? Yes No

Recommendation: As with other exterior doors in the home, it is important that the basement door be of solid core wood or steel construction and equipped with a quality deadbolt lock to prevent entry by intruders.

4. Can the interior of the home be accessed through windows or other openings from the second floor or roof? Yes No

Recommendation: All second floor windows and roof skylights must be secured to prevent access by intruders who could use drainpipes and other means to access the roof or upper floors.

5. Does the home have louver-type windows? Yes No

Recommendation: Louver windows should be replaced with solid windows made with tempered or shatterproof material.

6. Do all windows have adequate window coverings? Yes No

Recommendation: Windows should be equipped with internal blinds, curtains, drapes, or shutters to prevent someone from seeing inside.

CONDOMINIUM AND APARTMENT SECURITY

Security in condominium and apartment complexes must be a cooperative effort between residents, management, maintenance workers, and police. All must work together to provide the best possible security for the building. Most of the recommendations for single-family dwellings apply to condominiums and apartment complexes. The following is an audit that is particular to those type buildings.

1. Do all doors and windows have locks that will secure the condominium/apartment while it is vacant? Yes No

Recommendation: Examine all locks on doors and windows to

ensure they are working properly. Before leaving the condominium/apartment, make sure all doors and windows are locked. Always double-check locked access windows that are at ground level.

2. Does your complex have a separate “Laundromat” area? Yes No

Recommendation: If at all possible, avoid using the Laundromat in your complex by yourself. Always team up with a neighbor who you know and trust.

3. Does your complex have a building association or a way to alert residents of an emergency? Yes No

Recommendation: Develop an apartment alert system with neighbors in the complex to help protect each other’s property. A well-organized and active tenant association will assist in deterring intruders.

Recommendation: Get to know the tenants in the complex. After you meet them, make a personal contact list for future use.

4. Does the complex have an electronic access system to control entry into the building? Yes No

Recommendation: Do not allow access to strangers by “buzzing” them into the building. If someone enters the building by following you in, and that person is unknown to you, do not ride the elevator with them. If needed, exit the building and then re-enter later.

Recommendation: Report suspicious strangers, sounds, or actions to police, then notify the complex manager.

MAIL SECURITY

If you receive mail at your home, be wary of suspicious letters or packages. Do not open a letter that appears to be unusual in any way, particularly if it has a perceptible bump, which might be an explosive device. Notify law enforcement immediately of any unexplained package in or near your home. You should notify law enforcement when mail items have any suspicious features, such as:

- Excessive weight, size, or postage
- Springiness in the top, bottom, or sides of the envelope
- Wires or strings protruding from or attached to the envelope
- Envelope has uneven balance or a peculiar odor

- Stiffening of an envelope with cards or other material (such stiffening could be a spring-loaded explosive striker)
- No return address or the place of origin is unusual or unknown
- Name is misspelled

All such items should be isolated. Only trained law enforcement professionals should be allowed to open suspicious mail.

FAMILY SECURITY RECOMMENDATIONS

Recommendation: If at all possible, your home telephone number should be unlisted.

Recommendation: Family members, including care givers, should never tell anyone you are out of the house. They should be instructed to only take messages from callers.

Recommendation: Emergency police and fire numbers should be programmed into the telephone using the “In Case of Emergency” (ICE) concept. If you do not have a programmable phone, you should post emergency numbers near the main telephone in the home.

Recommendation: Do not discuss family plans with outsiders. Even your friends should not be informed. In general, do not discuss your family’s comings and goings.

Recommendation: Family members should not stop at the same supermarket at the same time on the same day each week. Vary your daily activities.

Recommendation: Children should be instructed not to open doors to strangers. All visitors should be viewed through a peephole with the door locked. Intercom systems should be used to aid in the identification of strangers.

Recommendation: If it is necessary to leave children at home, keep the house well-lighted and notify the neighbors.

Recommendation: Advise your children to:

- Never leave home without advising parents where they will be and who will accompany them.
- Travel in pairs or groups.
- Walk along busy streets and avoid isolated areas.
- Use play areas where recreational activities are supervised by responsible adults and where police protection is readily available.
- Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot — even if the strangers say mom or dad sent them or said it was okay.

- Report immediately to the nearest person of authority (teacher or police) anyone who attempts to molest or annoy a child.

Recommendation: Be wary of strangers. Be watchful of strange cars that seem to cruise the neighborhood or strange persons who suddenly start to frequent the neighborhood streets. Record information that may be helpful to police.

Recommendation: Observe cars parked in the neighborhood with one or more persons inside or persons who seem to be doing nothing in particular.

Recommendation: Never reveal to any stranger that you are home alone.

Recommendation: Know where your children are at all times. Maintain a daily itinerary and stress the importance of notifying other family members of changes in the schedule.

Recommendation: As mentioned above, have unlisted telephone numbers for ALL family members.

Recommendation: Always request salesmen, repairmen, meter readers, delivery personnel, and even policemen (in civilian clothes) to show their identification prior to admitting them into your home. If in doubt about their identity, place a call to their business to confirm employment. Never accept a phone number that they offer; always use the telephone directory or call the information operator.

Recommendation: Do not put your home telephone number on stationary or on any name and address stickers in order to preclude undesirable telephone calls.

Recommendation: When harassing or obscene telephone calls are received, take action to change your phone number immediately. Family members should never engage in a telephone conversation with unknown or unidentified persons.

Recommendation: Children must follow a school schedule, but if they are driven to school, varied routes should be followed. Children should be escorted to and from bus stops. Neither hiking nor walking to school is recommended.

Recommendation: Inform school authorities that children should not be released from school, athletic events, and club meetings on the strength of a telephone call. Advise the school authorities to confirm the call with your home or office.

Recommendation: Instruct the school administration that if an authorized person does not explain a child's absence from school shortly after school starts, they are to call the child's home or your office to determine the child's status.

Recommendation: Do not open doors to strangers or accept delivery of packages unless the sender is known. Instruct children and in-home help on this procedure. Install a chain

lock on the main entry door so that you may accept small packages or letters by partially opening the door. Do not rely heavily on this type of lock, as an intruder can break them away by forcing the door.

Recommendation: Check references of service personnel, domestics and childcare providers, and any other employees who have routine access to your residence or property.

Recommendation: When receiving a wrong number telephone call, never give your name or number. Just state that the caller has the wrong number.

Recommendation: When a stranger requests to use your telephone for an emergency, never allow entry into the home. Offer to summon assistance, and use the phone yourself.

Recommendation: Never answer your telephone with your name; a simple hello is acceptable.

Recommendation: Report all suspicious activity to the local police.

TRAVEL RECOMMENDATIONS

Whether you are going to the store or Europe, the fact that you have left your home or office changes your security status **SIGNIFICANTLY**. Travel decreases your security because you are not adhering to your routine, but instead, you are exposed to unfamiliar surroundings. If you plan to travel outside your home area or overseas, you should check with your director of security for additional security measures that can be taken to protect you and your family.

VEHICULAR TRAVEL RECOMMENDATIONS

Recommendation: Do not pick up strangers or give a ride to a stranger or volunteer your car to a group of strangers even though you may have a friend with you in the car.

Recommendation: If you should have car trouble on the road, drive to the side of the road and place a handkerchief or white cloth on the radio antenna or door facing traffic. Either place a cell phone call or wait for help to come.

Recommendation: If you are driving and an attempt is made to force you off the road, move toward the center of the roadway and quickly proceed to a busy street and seek assistance. As you proceed, blow your horn to attract attention to your plight.

Recommendation: Do not stop to aid other motorists or pedestrians, regardless of the circumstances. If you believe the emergency is genuine, use a cell phone or proceed to a public phone and report the matter to authorities, then let them handle the emergency.

Recommendation: If you suspect you are being followed:

- Circle the block to confirm the surveillance.
- Do not stop or take other actions that could lead to a confrontation.
- Do not drive home.
- Do not try to evade or elude the follower.
- Obtain a description of the vehicle and its occupants.
- Go to the nearest police or fire station and report the incident.
- Have an alternative safe place to go in the event you cannot get to the police station.
- Report the incident to police once you are safe.

Recommendation: Avoid using magnetic key boxes hidden in the wheel well of your car.

Recommendation: Park your car in a secured garage; do not park your car on a public street.

GENERAL SECURITY RECOMMENDATIONS

Recommendation: Place the police emergency telephone number (911) and the police non-emergency number next to the phone in your home for immediate use; program it into your telephone system if possible. Do not answer the telephone with your name or official title.

Recommendation: Ladders and scaffolding should be kept in locked outbuildings or garages.

Recommendation: Advise the local police department of your occupation and address. Complete and submit a judicial profile for you and your family (attached), to the chief security officer for use in emergencies. Judicial profiles should be protected as “confidential-restricted access” documents.

Recommendation: Consider moving all fuse and switch boxes into the home if possible. Place locks on those that remain outside or in outbuildings/garages.

Recommendation: Consider a trained watchdog for the family residence. In addition to being a natural deterrent, it is another means of alarming the home.

Recommendation: Be constantly aware of surveillance. Usually a potential victim is watched for several days before an act of violence is carried out.

Recommendation: Prepare an inventory of household and personal possessions, describing the articles and listing the serial numbers for reference.

Recommendation: In order that personal items (jewelry, appliances, TV sets, radios, etc.) can be identified if lost or stolen, a code number should be engraved on each item with an etching machine.

Recommendation: A small safe or security box, which can be bolted down to a closet floor, should be used to secure personal jewelry, cash, and personal documents that are frequently used. Consider a safety deposit box for items used less frequently.

Recommendation: When the home is left vacant, install timers on televisions, radios, and lights in order to give the impression that the home is occupied.

Recommendation: Have “Caller ID” for incoming telephone calls to your home. Use “Caller ID” blocking to prevent your telephone number from being displayed on outgoing calls.

Recommendation: Become familiar with the streets and roads surrounding your home. Have a planned escape route from your home to a designated safe place in case of fire or intrusion.

Recommendation: Plan and practice driving to area emergency services, such as hospitals, police stations, and safe places.

Recommendation: Make sure your trash is kept in a secure place, such as a locked outbuilding.

Recommendation: Keep the names, addresses, and telephone numbers for all staff members handy in the event of an emergency.

Recommendation: If you have household employees, make sure they have been screened with background checks.

**For further information contact:
National Center for State Courts
Court Consulting Services
707 17th Street – Suite 2900
Denver, CO 80202
(303) 305-4315**



This document was prepared by Jim O’Neil, NCSC Consultant

Revised: February 2009

Appendix D

Model Disaster Recovery Plan Forms

The following section presents sample forms that can be used for the development of a disaster plan regarding the preservations of electronic and hard copies of records in a state court system. The samples contained herein could be made part of pre-service for new employees and in-service training for court staff.

Disaster Planning and Recovery Worksheets

Worksheet Name	Content of worksheet and Instructions	Page
	<p>PRE-DISASTER DOCUMENTATION A set of worksheets should be completed for each court location. This set should be updated annually.</p>	
Emergency Telephone List	Telephone contact for persons and agencies that must be notified of the event	
Disaster Team Assignments	List of names and 24-hour contact information for court disaster team members	
Equipment Supply List	Emergency supplies and equipment	
External Equipment Contacts	24-hour contact information for vendors or others who are able to supply resources or equipment	
Floor Plan	Diagram of the court and/or vault annotated to show the location of computer equipment as well as records	
Records Environment Risk Assessment	A survey of the building, inside and out, especially noting leaks, broken windows and doors, dirt, extraneous materials, damaged furnishings, and other potential hazards	
Evacuation Plan	Security plan to evacuate building, a fundamental part of the court's COOP	
Records Inventory	Inventory of court and administrative records in the area – both electronic and hard copy – including record series titles and dates	
	<p>DISASTER RESPONSE DOCUMENTATION These worksheets are completed during the recovery and salvage process.</p>	
General Procedures During a Disaster	A list of steps to be taken when a disaster occurs for the recovery of both electronic records and hard copy	
Damage Assessment Report	A report used to determine salvage priorities that is composed of a description of the problem created immediately after the event, including an estimate of the scope of the damage, the records involved, and the magnitude of the damage	
Priority Listing	Listing of records to be treated, arranged by priority	
Interim Inventory	A list of the new location of records removed from the usual location for treatment, a list that must be updated as records are treated and returned or marked as unsalvageable	
Disaster Log	Chronological record of actions taken, records involved, and responsible individuals	

Emergency Telephone Numbers

Date completed _____

Form completed by _____

Agency	Contact and alternative if needed	Telephone Numbers
Court Administration		
Police		
Fire Department		
Medical Assistance		
Ambulance		
Other Government Officer		
Maintenance Training and Security Company		
Internet Service Provider		
Judiciary IT Services		
Judicial Security Services		
Disaster Team Leaders		

Disaster Team Assignments and Responsibilities

Date completed _____

Location _____

Team Member Name	Title	Responsibilities	Contact Information
	Team Leader(s)	Individuals with authority to make decisions and to direct others during the disaster and salvage operations. Assign tasks to individuals; perform priority assessment, direct contacts with outside authorities and vendors. Supervise recovery. These individuals are responsible for pre-disaster planning and disaster manual completion for a courthouse. Responsible for the safe evacuation of the building and identification of the location of vital records, both electronic and hard copy.	
	Backup Team Leader(s)	Serves as a back up to the team leader(s) responsible for carrying out leader functions in the absence of the leader. Must have a thorough knowledge of the plan and the resources available.	
	Team Recorder	Team member responsible for completion of logs and documents describing the actions undertaken during the disaster assessment and recovery process. This team member is responsible for annotating the movement of records from disaster site to temporary repair location and return.	
	Team Communications Officer	Responsible for communicating information to judges, court personnel, and outside media regarding the status of recovery and the extent of damage of electronic and hard copy records.	
	Team Member	Responsibilities as assigned.	
	Team Member	Responsibilities as assigned.	

External Vendor Contact Information

Date _____

Function or Procedure	Name and Address Contact Person	Telephone or Emergency Access Number
Transport - trucks and equipment to transport boxes of records and/or computer equipment		
Freezer or cold storage location for hard copies		
Freeze-drying contractor for hard copies		
Portable generators to borrow or lease for backup electricity		
Food services (for workers)		
Refrigerated trucks		
Conservationist		
Pest control		
Fumigation services		
Salvage services		
Trash removal		
Alternative location for air drying		
Electrical contractors		
Computer restoration experts		

General Procedures for Hard Copy Records Recovery and Salvage

1. Make sure persons are safe and out of the area.
2. Notify the appropriate persons and agencies of the event. DO NOT try to re-enter a building or handle records until the police and/or fire department indicate that it is safe to enter. Notify the disaster team and administrative officers.
3. Create an assessment report that describes the damage to the structure and materials.
4. Do not remove any records from the area until the priority plan is complete.
5. Create a priority assessment listing the sequence of steps to be taken.
6. Identify a location where records recovery work can take place.
7. DO NOT TRY TO REPAIR RECORDS IN THE DISASTER AREA. All records must be removed to avoid the possibility of additional damage.
8. Try not to exacerbate the damage during the removal process.
9. Document the records being removed. Label the floor plan and note on the disaster log the record type and date, original location, and location in the recovery area.
10. Salvage damaged materials appropriately according to the type of damage.
11. Repair the damaged location.
12. Return materials to the damaged area after inspection.
13. Maintain a disaster log describing actions for future reference.
14. Prepare a disaster report summarizing the event; include advice and analysis of procedures.
15. Replace any emergency equipment or supplies.

Floor Plan

The floor plan of the court should be available in electronic format and in hard copy to help rescue personnel and other professionals physically respond to a disaster or emergency. It should help identify potential problems in addition to providing an overview of the physical layout as well as the location of outlets, master switches, vaults, staircases, windows, and computer equipment. The locations of records, especially confidential and sealed records, should be noted on the plan. The floor plan should be updated annually and copies kept with first responders.

Appendix E

Unified Judicial System of Pennsylvania Security Incident Fact Sheet

UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA
Security Incident Fact Sheet

DISTRICT 02-1-01
DATE OF INCIDENT March 18 2005
TIME OF INCIDENT Hour Minutes a.m.

Check Boxes Only Where Applicable

WHAT WAS THE NATURE OF INCIDENT?:

You may choose multiple items from each area below.

You may enter another type of incident by typing a 2- or 3-word description in the "Other" box.

Personal		
<input type="checkbox"/> Disorderly Person(s)	Other (Describe below)	
<input type="checkbox"/> Physical Assault	<input type="text"/>	
Threat		
<input type="checkbox"/> Bomb	Other (Describe below)	
<input type="checkbox"/> Suspicious Package	<input type="text"/>	
<input type="checkbox"/> Verbal		
Threat Mode		
<input type="checkbox"/> Direct Contact		
<input type="checkbox"/> E-mail	Other (Describe below)	
<input type="checkbox"/> Mail	<input type="text"/>	
<input type="checkbox"/> Telephone		
Property Damage		
<input type="checkbox"/> Arson	Other (Describe below)	
<input type="checkbox"/> Theft	<input type="text"/>	
<input type="checkbox"/> Vandalism		
Drugs		
<input type="checkbox"/> Drugs or Contraband	Other (Describe below)	
	<input type="text"/>	
Emergency		
<input type="checkbox"/> Contamination Exposure	<input type="checkbox"/> Medical	Other (Describe below)
<input type="checkbox"/> Explosion	<input type="checkbox"/> Prisoner Escape	<input type="text"/>
<input type="checkbox"/> Fire	<input type="checkbox"/> Weather	

WHAT WAS THE EXTENT OF INJURIES?:

- None
- Don't know
- Minor
- Medical attention required

Description of injuries:

WEAPON INVOLVED?:

You may choose multiple items and/or provide other description.

- None
- Box cutter
- Hands/feet
- Razor blade
- Biological agent
- Chemical agent
- Knife
- Rifle
- Blunt object
- Handgun/pistol
- Pepper spray
- Shotgun

Other: (Describe weapon(s) at right)

IN RELATION TO THE MAGISTERIAL DISTRICT JUDGE COURT FACILITY, WHERE DID THE INCIDENT OCCUR?:

You may choose multiple items and/or provide other description.

- Central Court
- Garage
- Grounds
- Staff area
- Chambers
- Hallway
- Lobby
- Courtroom
- Holding cell
- Parking lot

- Off-site. Indicate address or location.
(Describe at right)

WAS AN ALARM ACTIVATED?:

- No
- Duress/Panic button
- Emergency call (911)
- Magnetometer/X-Ray

Other: What agencies were notified?

WHO WAS INVOLVED IN THE INCIDENT?:

You may choose multiple individuals and write in any not listed.

- Magisterial District Judge
- Prosecutor
- Security officer
- Defendant
- Court Staff
- Constable
- Sheriff
- Plaintiff
- Defense counsel
- Municipal police
- State police
- Prisoner
- Member of public

Other (Describe at right)

Were any of the persons involved in the incident attending a court proceeding? Yes No

If yes, what type of case?

- Civil Case Landlord/tenant Private Criminal Complaint Non-traffic Citation
 Criminal Case Protection From Abuse Traffic Citation

Case Caption (Enter at right)

If known, enter names of those involved. Enter number of names then click update.

Update

SUMMARY OF FACTS:

Please include the name of each agency that responded to the incident (e.g., sheriff, state police, fire department) as well as the circumstances leading up to the event.

NAME OF INDIVIDUAL FILING THIS REPORT:

Larry C. Kerr

Did you personally witness the incident? Yes No

If you answered No above, enter the name of the person for whom you are filing this report:

Last name:

First name:

Middle initial:

Name suffix: (Jr., Sr.)

REPORT FILING OPTIONS

Save until I return and complete the report

(Allows you to return and edit this report within the next 7 days. This option is useful if you cannot complete the report at this time.)

Save and return

OR

Save the report for the record

(This option will submit the report immediately. You will not have the option of editing this report at a later time.)

Save for the record

Appendix F

Sample Memorandum of Understanding

**MEMORANDUM OF UNDERSTANDING
BETWEEN
THE (Name of County/Parish)
AND
(Name of Court)**

FOR A TEMPORARY COURT SITE IN THE EVENT OF DISASTER

This Memorandum of Understanding is made and entered into on the ___ day of (month), 20___, by and between the County/Parish and the Court.

- (1) The County/Parish hereby recognizes the need for the preservation of access to justice for all citizens, judicial efficiency and judicial responsiveness, public health, safety and welfare afforded the citizens of this County/Parish as is necessary to respond to the needs of the public in the event of a disaster to the Court building , located at (address) .
- (2) Certain space and equipment within the (title of building[s]), located at (address), shall be made temporarily available for use by the Court in the event the Court Building is seriously damaged and/or destroyed in an event primarily isolated to the Court building and not a County/Parish-wide disaster or emergency event.
- (3) The Court shall have the use of courtroom(s) (building[s]) to be designated if the need arises.
- (4) Any equipment owned by the County/Parish may be used by the Court and its employees subject to the security and operating rules and regulations of the County/Parish.
- (5) All employees working for or with the judges of Court shall remain Court employees.
- (6) The day-to-day Court management activities shall be under the direction and control of one Court employee or judge designated by the Court to serve as its "Judicial Administrator". This person shall be responsible for the day-to-day administrative oversight, control, and guidance of all aspects of the use of the County/Parish property and equipment under this Agreement.
- (7) The Court is permitted to deliver for its own exclusive use such chairs, desks, and computer equipment as is necessary to properly function.

- (8) The Court shall be responsible for all maintenance, upkeep, repairs and technical and engineering assistance on its own equipment during the term of this Agreement. The Court shall also be responsible for the maintenance, upkeep and repair of County/Parish equipment they may use, beyond normal wear and tear, provided that the County/Parish equipment is used exclusively and/or primarily by the Court.
- (9) The Court is entitled to remove and shall remove all of its movable equipment from the building at the termination of this Agreement. The County/Parish shall have no claim or interest in any movable that is owned by the Court.
- (10) The Court's movables shall be insured at its own expense.
- (11) The Court will arrange for courtroom security as is customary for its day-to-day operations at the Court's expense.
- (12) Any additional costs incurred by the County/Parish to house the Court such as, but not limited to, water, gas, and electricity, will be reimbursed to the County/Parish from the Court's adopted budget.
- (13) The Court will be responsible for any damages of any nature deemed as more than normal wear and tear.

TERMINATION

This agreement may be terminated by either party at any time within thirty (30) days written notice or as otherwise stated herein. All notices shall be sent to the undersigned parties by certified mail, return receipt requested.

REMEDIES FOR DEFAULT

Any claim or controversy arising out of this agreement shall be resolved as per law. Venue and jurisdiction shall be the (designate jurisdiction) .

ASSIGNMENT

No party herein shall assign any interest in the same (whether by assignment or notation).

TERM OF AGREEMENT

This Agreement shall remain in full force and effect unless terminated by one or both of the parties to this Agreement.

DISCRIMINATION CLAUSE

The County/Parish and Court agree not to discriminate in their respective employment practices, and will render services under this Agreement without regard to race, color, religion, sex, national origin, veteran status, political affiliation, disabilities.

INDEMNIFICATION

The Court and County/Parish both agree to indemnify, hold harmless and defend each other, and their respective officers, agents, servants, attorneys and employees from and against any and all claims, demands, losses, suits, damages, judgments, costs and expenses whether, indirect or consequential and including but not limited to all fees, expenses and charges of attorneys and other professionals, as well as court costs and expenses, for actions or inactions arising out of, in connection with or resulting from the use of the (building identified above) hereinafter arising from claims or violations resulting from such usage in the course and scope of this Agreement for any employee and/or loaned employee that may be due to and caused in whole or in part by any act, error, or commission or commission of any act by negligence or otherwise while performing services.

SEVERABILITY

If any term or clause herein is deemed unenforceable or invalid for any reason whatsoever, then that portion shall be severable and the remainder shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Agreement as of this ____ day of (month),____, 20__.

County/Parish

Court

By _____

By _____

WITNESS:



Guidelines for Implementing Best Practices in Court Building Security

**Costs, Priorities,
Funding Strategies, and Accountability**

**A Paper by the National Center for State Courts
Funded by the State Justice Institute
Grant Number SJI-09-P-125**



© 2010
National Center for State Courts

This document was prepared under State Justice Institute (SJI) Grant SJI-09-P-125. The points of view and opinions expressed in this document are those of the author, and they do not necessarily represent the policy and positions of the State Justice Institute. The National Center for State Courts grants the State Justice Institute a royalty-free, non-exclusive license to produce, reproduce, publish, distribute or otherwise use, and to authorize others to use, all or any part of these documents for any governmental or public purpose.

Table of Contents

	Page
Acknowledgements	
Introduction.....	1
Part One: Costs of Courthouse Security Improvements	3
Part Two: Spending Priorities.....	9
Part Three: Funding Best Practices: Strategies for Working with Stakeholders	16
Part Four: Accountability and Performance Measures	23
Appendix.....	30

Acknowledgements

The development and publication of this report has been made possible by the continued cooperation and hard work of many people. The National Center for State Courts (NCSC) wishes to thank the State Justice Institute, who provided the funding that made this project possible. The security team of Timm Fautsko, Principal Staff at NCSC, and NCSC security consultants Steve Berson, Jim O’Neil, and Kevin Sheehan, is primarily responsible for this report and the previous development of the “Steps to Best Practices in Court Security” contained in Appendix A. Further, their work in identifying costs of these best practices has provided a useful guide for the acquisition of security staff and equipment to improve court security and public safety at local and state levels. A special thank you from the security team is extended to those members of the project’s advisory committee who reviewed this publication and made important recommendations to improve the final product. Their many years of experience in the field of court security and emergency preparedness proved invaluable in *reality testing* not only the cost acquisition information, but the many steps to best practice. Without their assistance, the quality of information contained in this report would not have been possible – Frank Lalley, Judicial Security Administrator, Pennsylvania; Malcolm Franklin, Senior Manager, Emergency Response and Security, California; and Carol Price, Court Security Director, Utah. Finally, the members of the NCSC security team want to thank both NCSC editorial staff Ephanie Blair and Lorie Gomez for the many hours they spent providing quality assurance in the conformation and final editing of the report.

Introduction

Operating a court building today is by its very nature a risky business. Day in and day out, court buildings are visited by a large volume of disgruntled and even lawbreaking citizens. Moreover, court buildings can be seen as an important symbolic target for those in our midst who wish to wreak mischief or terror.

In an effort to assist courts in the development and implementation of effective measures for court building security, the National Center for State Courts (NCSC) has developed *Steps to Best Practices*. This document, attached as the Appendix, sets forth guidelines for what constitutes best practices in various areas of court building security. It also sets forth steps in phases that can be taken toward achieving these best practices. These steps may be a useful approach for courts as they strive to prioritize and implement additional improvements in court building security. The NCSC wishes to emphasize that a fully effective integrated level of security will be reached only when all the measures at the best practices level are incorporated. Recognizing that these measures at the best practices level can at times be costly, the *Steps* document provides these steps in phases, so that a court at its discretion can adopt incremental improvements before reaching the level of best practices. These steps in phases are plateaus along an ascending path to improvement – improvement that can be achieved by a court over time.

To further assist courts in working with the *Steps* document, the NCSC has prepared this paper funded by the State Justice Institute. This paper includes four parts:

Part One identifies the estimated costs associated with implementing the recommendations contained in the *Steps* document.

Part Two includes a framework of priorities that a court may wish to follow in deciding when and how to implement the recommendations contained in *Steps*.

Part Three recommends strategies for seeking the funds necessary to implement the recommendations contained in *Steps*.

Part Four describes performance and accountability measures that a court may wish to utilize in order to measure the effectiveness of implementation efforts and to sustain funding for those efforts.

Court building security is not a one-time achievement. It is a serious and continuous goal and requires constant vigilance. Further, it must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and they can never be eliminated. With proper attention and care, however, they can be minimized. Following the recommendations in the *Steps* document, along with the guidance provided in the four parts of this paper, can help courts minimize the risks and help keep the public, court staff, building tenants, and judicial officers more safe and secure.

Part One **Costs of Courthouse Security Improvements**

The purpose of Part One is to identify the costs associated with implementing the recommendations contained in the NCSC's *Steps to Best Practices*. Almost all of the topics in the *Steps to Best Practices* document include recommendations that will require courts to spend funds on equipment or staff. These costs are set forth below by topic.

It is important to note at the outset that the costs identified here are estimates only. Costs for equipment are based on price ranges listed in catalogues, including those catalogues found through the website of American Society for Industrial Security (ASIS) International, an organization of security professionals that includes law enforcement and court security officials. The cost of equipment may vary based on brand, model, and dealer or distributor. Quantity discounts may be available through the use of county or state purchasing agreements with one or more vendors, based on the number and types of items covered by a particular order. Costs are current as of the publication of this paper.

It is important to note that in many cases the cost of installing equipment can be significant in relation to the cost of acquisition. Such installation costs are not included in the amounts indicated below and will need to be determined at the state or local level on a case-by-case basis.

The most frequently mentioned items in this analysis requiring expenditures are: (a) court security officers (CSOs) and (b) electronic systems for closed circuit television (CCTV) cameras, duress alarms, and door access systems. Costs for these items are set forth with specificity in Table A. Costs for all other referenced items are set forth by topic in Table B. When any topic listed in Table B includes expenditures for CSOs, or for CCTV, duress alarms, or door access systems, there will be a cross reference to the specific costs for these items as included in Table A.

Finally, not all courts will find their actual costs falling within the ranges indicated in the tables below. There will inevitably be outliers. A good example of this is the case of deputy sheriffs or court security officers. As noted below, the ranges indicated for these staff positions are derived from the Bureau of Labor Statistics. These ranges are calculated by the Bureau using a methodology that in effect disregards data points that fall lower than the tenth percentile or higher than the 90th percentile.

Accordingly, some larger jurisdictions, for example, may face staffing costs that exceed the higher end of the range indicated.

Table A

Item	Estimated Cost
Topic A-1: Court Security Officers (CSOs)	
County Sheriff Deputies	\$30,100 - \$79,700
Annual salary based on 2008 data from the Bureau of Labor Statistics. This represents a range around the national median (\$54,100) from 10% at the low end to 90% at the high end.	
State Court Security Officers	\$18,700 - \$61,500
Annual salary based on 2008 data from the Bureau of Labor Statistics. This represents a range around the national median (\$37,800) from 10% at the low end to 90% at the high end.	
Topic A-2: CCTV Camera Systems	
These systems include color, digital, and recording capacity.	
Tilt/Pan/Zoom – exterior camera, including housing and mounting units	\$1,500 - \$1,800
Tilt/Pan/Zoom – interior camera, including housing units	\$1,200 - \$1,500
Fixed – exterior camera, including housing and mounting units	\$400 - \$600
Fixed – interior camera, including housing units	\$250 - \$400
Digital video recorder (DVR) – 16 channel input	\$3,000 - \$5,000
Digital video recorder (DVR) – 32 channel input	\$5,000 - \$8,000
Flat-screen monitor 17-inch	\$500 - \$800
Flat-screen monitor 40-inch	\$2,500 - \$3,000
Topic A-3: Duress Alarm Systems	
These systems can be either hard-wired or wireless.	
Alarm control panel (hard-wired)	\$250 - \$300
Alarm control panel (wireless)	\$250 - \$300
Panic button (hard-wired)	\$50 - \$75
Panic button (wireless)	\$75 - \$125
Remote receiver (wireless)	\$550 - \$650
Alarm sirens (for either hard-wired or wireless system)	\$50 - 75
Alarm strobe lights (for either hard-wired or wireless system)	\$25 - \$35
Topic A-4: Access Card Systems	
Control panel	\$900 - \$1,200
Card reader, per door	\$500 - \$600
Software to operate system	\$1,200 - \$1,500
Magnetic lock, per door	\$250 - \$350
Emergency exit button, per door	\$40 - \$60
Computer and printer (if no other such equipment is available in the court building for this system)	\$600 - \$800

Table B

Item	Estimated Cost
Topic B-1: Access of People into Court Building	
Magnetometer: single-zone units will be on the lower end of the range; multi-zone units will be at the higher end.	\$2,200 - \$8,600
X-ray machine	\$15,000 - \$35,000
Hand-wands	\$200 - \$300
Court security officers (CSOs)	See Table A
Electronic access card system	See Table A
CCTV cameras	See Table A
Lock box for weapons (four compartments)	\$350 - \$400
Topic B-2: After-hours Access	
Electronic access card system	See Table A
Background checks: national check of criminal history and motor vehicle history. There is no charge for in-house certified user of National Crime Information Center (NCIC) or Criminal Offender Record Information (CORI).	
Topic B-3: Chambers	
Duress alarms	See Table A
Window coverings: cellular shades (24" x 36")	\$55 - \$65
Window coverings: vertical blinds (24" x 36")	\$110 - \$130
CSOs	See Table A
CCTV	See Table A
Ballistic-resistant material for windows	May require bids
Topic B-4: Courtrooms	
CSOs	See Table A
Duress alarms	See Table A
CCTV	See Table A
Ballistic-resistant material	May require bids
Video arraignment	May require bids
Topic B-5: CSO Staffing Level	
CSOs	See Table A
Topic B-6: Duress Alarms	
Duress alarms	See Table A

Topic B-8: In-custody Defendants	
CSOs	See Table A
CCTV	See Table A
Sally port	Will require bids
Secure pathway	Will require bids
Topic C-1: Closed Circuit Television (CCTV)	
CCTV	See Table A
Topic C-2: Emergency Equipment and Procedures	
Emergency generators, battery-operated, for backup lighting in courtrooms and other specific areas	\$325 - \$375
Fire alarm – horn and strobe light	\$45 - \$55
Fire extinguisher (ten pound commercial brand)	\$65 - \$75
Elevators to code	Will require bids
Emergency generator for court building	Will require bids
Voice-activated fire notification system – wireless, per unit	\$325 - \$375
CCTV	See Table A
AED	\$1,700 - \$1,800
Topic C-3: Interior Access	
Electronic access card system	See Table A
Viewing ports	\$150 - \$300
CCTV	See Table A
Videophone	\$350 - \$700
Topic C-4: Intrusion Alarms	
Door contacts	\$70 - \$80
Passive infrared motion detector strip	\$90 - \$110
Glass-break sensors	\$70 - \$80
Control panel	\$225 - \$275
CCTV	See Table A
Topic C-5: Jurors	
CSOs	See Table A
Topic C-6: Parking	
CSOs	See Table A
Electronic access card system	See Table A
CCTV	See Table A
Security fencing (chain link with security slats, priced per 8' x 8' section)	\$1,200 - \$1,300

Topic C-7	
Duress alarms	See Table A
CCTV	See Table A
CSOs	See Table A
Plexiglas-type enclosures, priced per square foot for 1¼-inch thick material	\$60 -\$65
Alarm for safe	\$75 - \$85
Topic D-1: Cash Handling	
Duress alarms	See Table A
CCTV	See Table A
CSOs	See Table A
Armored courier service	May require bids
Topic D-2: Exterior/Interior Patrols	
CSOs	See Table A
Topic D-3: Perimeter Issues	
Lighting	
Wall pack mount (9" x 18")	\$200 - \$220
Pole unit (16-inch)	\$275 - \$325
High-pressure sodium bulbs	\$60 - \$70
Intrusion alarm	
Door contacts	\$70 - \$80
Passive infrared motion detector strip	\$90 - \$110
Glass-break sensors	\$70 - \$80
Control panel	\$225 - \$275
Bollards	
Round carbon steel – 48-inch	\$1,200 - \$1,300
Concrete with welded rebar – 48-inch	\$375 - \$425
Security fencing (chain link with security slats, priced per 8' X 8' section)	\$1,200 - \$1,300
CCTV	See Table A
CSOs	See Table A
Electronic access card system	See Table A
Topic D-4: Lobbies, Hallways, Stairwells, and Elevators	
CCTV	See Table A
CSOs	See Table A
Emergency lighting, per unit	\$325 - \$375
Public address system – emergency alert intercom system	\$10,000 - \$15,000

Topic D-5: Screening Mail and Packages	
Magnetometer: single-zone units will be on the lower end of the range; multi-zone units will be at the higher end.	\$2,200 - \$8,600
X-ray machine	\$15,000 - \$35,000
Off-site screening station	Will require bids

Part Two **Spending Priorities**

As court leaders, court administrators and judges face a great responsibility and challenge in providing a safe and secure environment for those who work in or visit court buildings. The staffing levels and equipment required to provide such an environment can be costly. More likely than not, the costs for establishing and maintaining a reasonably sufficient level of court building security will exceed the amount of funding available.

Accordingly, court leadership must consider priorities very carefully when making spending decisions with respect to court building security. They will need to ask themselves: “How do we spend limited funds on security so that we get the most ‘bang for the buck?’ What security measures should we put in place first, what comes next, and what measures can wait until later?”

The NCSC’s *Steps to Best Practices* document provides guidance with respect to spending priorities in two ways. First, it organizes topics into the following priority categories: fundamental, extremely important, very important, and important. Second, within each topic, action steps and phases are listed and recommended in priority order. While this document recommends priorities, there is no prescription for spending priorities. Court administrators, in the end, must set forth their own formula for determining the order in which items will receive security funds.

Indeed, it may not be feasible to provide a precise prescription or formula when it comes to spending priorities for court building security. Each court building is designed differently and faces a unique set of needs and resources that must be taken into account when determining the priority of security spending. In the final analysis, rather than following a rigid formula, court leadership will need to rely on its own judgment as to what is best for its court building.

It may be possible, however, to provide general guidance on priorities. This paper presents a conceptual framework that court leadership may find helpful in determining a priority order for spending on security. This conceptual framework relies on the information contained in *Steps to Best Practices* and provides a way for courts to weave

that information into a meaningful spending plan for court building security. This conceptual framework revolves around the following four goals:

- **Goal #1 – Prepare a proper foundation for court building security.**
- **Goal #2 – Prevent dangerous items and/or dangerous people from entering the court building.**
- **Goal #3 – Have the capacity to react quickly and effectively to any security incident that occurs within or around the court building.**
- **Goal #4 – Have the capacity to prevent or minimize the risk of a security incident occurring within or on the outside of the court building.**

Goal #1 – Prepare a Proper Foundation

A spending plan for court building security can be meaningful only if it is based on a solid foundation that includes a robust needs analysis. In terms of security, court leadership must have a fundamental understanding of the following: What are the risks? What are the security measures already in place? What are the significant gaps in security protection that must be put into place?

Answers to these fundamental questions can be garnered by putting into place the recommendations described by the topics under “Category A: Fundamental” in *Steps to Best Practices*. These topics are a security committee, policies and procedures, and a command and control center.

The establishment of a security committee will provide the court the wherewithal to carefully assess its security needs and determine next steps, including the development of a spending plan. Creating policies and procedures will further refine the court’s direction for security protocols and enforcement and subsequent spending needs. Once these fundamentals are in place, Goal #1 is achieved. The court is ready to move forward on spending priorities relating to the remaining goals, relying on its own needs analysis along with the guidance contained in *Steps to Best Practices*.

Goals # 2 through #4 – Addressing Security Needs

Guidance from *Steps to Best Practices* in addressing Goals #2 through #4 can take different forms. All efforts will, in reality, need to be incremental. No goal will be fully satisfied initially, nor will best practices likely be achieved at once for any of the topics in

Steps to Best Practices. The incremental approach recommended here relies on the following three guidelines:

- Address the priority sequence of the goals. Do some work on Goal #2 first, then Goal #3, then Goal #4.
- Address the priorities reflected in the *Steps to Best Practices* categories. Look to the relevant topics first in category B (extremely important), then C (very important), and then D (important).
- Follow the priority sequence of the steps within each topic. Try to achieve one or more of the phases along the way to best practices within each topic.

Following this approach, court leadership will determine, based on its needs assessment, a reasonable level of additional effort it is able to make toward achieving Goal #2. It will do the same for Goals #3 and #4 consecutively. This reasonable level of effort will consist initially of taking a certain number of steps in all of the “extremely important” *Steps to Best Practices* topics relating to each goal. Court leadership will then take steps in the “very important” topics relating to each goal, then in the “important” topics relating to each goal. Once court leadership has accomplished this, it will have achieved a certain level of court building security, even though it may not have achieved the “best practices” level in any topic.

Sequence for Addressing Goals #2 - #4

	<u>Goal #2</u> Access Control	<u>Goal #3</u> Capacity to React	<u>Goal #4</u> Capacity to Prevent
<u>Category B</u> Extremely Important Topics	First Spending Priority	Second Spending Priority	Third Spending Priority
<u>Category C</u> Very Important Topics	Fourth Spending Priority	Fifth Spending Priority	Sixth Spending Priority
<u>Category D</u> Important Topics	Seventh Spending Priority	Eighth Spending Priority	Ninth Spending Priority

Over time, and as additional funds become available, a court can repeat the effort. Starting again with Goal #1, it can reassess its current situation. Then it can go further

toward best practices for all the extremely important topics relating to Goal #2, #3, and #4 consecutively. It can go further toward best practices in the topics for the very important and important categories as well.

To illustrate this approach, in addressing Goal #2, a court will need to decide what actions it must take to keep the court building free of all unauthorized weapons or any other items that can cause injury to people or harm to property. The risk of an attack inside the court building by someone with a gun or other weapon, and the risk of explosives being set off inside the building are real and extremely serious. Expenditures of funds on staff and equipment are required to mitigate these risks.

Steps to Best Practices includes several topics relating to Goal #2. Each of these topics contains steps that will assist the court in pursuing the goal of keeping the court building free from weapons and hazardous materials. To determine funding priorities in pursuit of Goal #2, a court will focus first on those topics within Category B, “extremely important.” These topics are: B-1, access of people; B-2, after-hours access; B-5, CSO staffing levels; and B-7, threat and incident reporting.

Relating Topics to Goals



The court should decide how far down the steps in each of those topics it can and should go. As an example, a court might decide that it will take all the steps required to achieve the second phase of topic B-1 and all the steps required to achieve the first phase of topic B-2. Again, there is no rigid formula. Each court needs to decide what is best, based on its own unique needs and capacity. However, it can rely on guidance on the

priorities embedded in *Steps to Best Practices*, focusing on the extremely important topics first and taking the steps within each topic in priority order.

Once the court has addressed the topics in the extremely important category relating to Goal #2, it is time to move on to Goal #3 and repeat the process. Goal #3 describes the capacity to effectively and quickly respond to incidents. *Steps to Best Practices* includes topics relating to Goal #3 in the extremely important category. These are: topic B-5, CSO staffing; topic B-6, duress alarms; and topic B-9, training. Each of these topics includes steps that will enhance the capacity of the court to respond to incidents. The court should focus on those topics in category B that will help achieve Goal #3. It should go through the steps and phases of these extremely important topics as far as it reasonably can.

Next, the court should move on to Goal #4, which encompasses preventing or minimizing the risk of serious incidents. The topics in the extremely important category relating to this goal include: B-3, chambers; B-4 courtrooms; B-7, threat and incident reporting; B-8, in-custody defendants; and B-9, training.

After all of the extremely important topics have been considered, the court can return to Goal #2 and address all of the Category C (very important) topics that relate to that goal. It can then address all the Category C topics that relate to Goal #3 and #4 consecutively. Finally, the court can address all of the Category D (important) topics that relate to Goals #2, #3, and #4 consecutively.

The approach described in this part is the one recommended by the NCSC. Courts may take differing approaches. Court leadership, however, should have some structured methodology in mind. It should set goals and have a good understanding of the priority of tasks required to achieve those goals. Based on its own assessment of the unique security challenges and opportunities it faces, court leadership may wish to reconfigure the description and priority sequence of the four goals discussed above. It may also wish to reconsider the priorities embedded in the *Steps to Best Practices*. This paper, as well as the *Steps to Best Practices*, is offered as a guide to court leadership. The priorities reflected in these documents are based on the extensive security experience of the NCSC assessment team and of its group of advisors.

The following table details the relationship to each of the four goals of the many provisions contained in the *Steps to Best Practices*.

Relationship of Topics to Goals

Goal #1: Preparing a Proper Foundation	
Category A: Fundamental	
A-1	Command and control center
A-2	Policies and procedures
A-3	Security committee
Goal #2: Preventing Dangerous Items and People from Entering the Court Building	
Category B: Extremely Important	
B-1	Access of people into the court building
B-2	After-hours access into the court building
B-5	Court security officer (CSO) staffing level
B-7	Threat and incident reporting
Category C: Very Important	
C-1	CCTV cameras
C-4	Intrusion alarms
Category D: Important	
D2	Exterior patrols
D-3	Perimeter issues
D-5	Screening mail and packages
Goal #3: Capacity to React Quickly and Effectively	
Category B: Extremely Important	
B-5	CSOs
B-6	Duress alarms
B-9	Training
Category C: Very Important	
C-1	CCTV cameras
C-2	Emergency equipment and procedures
Category D: Important	
D-2	Exterior/interior patrols

Goal #4: Preventing or Minimizing the Risk of Security Incidents	
Category B: Extremely Important	
B-3	Chambers
B-4	Courtrooms
B-7	Threat and incident reporting
B-8	In-custody defendants
B-9	Training
Category C: Very Important	
C-1	CCTV cameras
C-3	Circulation zones
C-6	Parking
C-7	Public counters and offices
Category D: Important	
D-2	Exterior/interior patrols
D-3	Perimeter issues
D-4	Public lobbies, hallways, stairwells, and elevators

Part Three

Funding Best Practices: Strategies for Working with Stakeholders

While in the final analysis courts may have ultimate responsibility for court building security, it is a responsibility that cannot be successfully discharged by courts alone. Courts acting on their own do not have the capacity or resources to fully address their own security needs. Cooperation and coordination with a host of other organizations is imperative. These other organizations are stakeholders who have a shared interest in court building security, to include the safety of their employees and the public they serve. Stakeholders may also have the capacity to help courts obtain the resources needed to make court buildings more secure. Many parties interested in the same issues and working together can serve to accomplish two significant goals for court building security:

- Developing a unified vision of what resources are needed to provide a reasonable level of security within and around a court building.
- Developing and executing a unified strategy for obtaining the resources needed.

Establishing a Security Committee

The key to getting stakeholders on board and working together is to develop and request their participation on an active and robust court building security committee. The establishment of a security committee is a fundamental recommendation in *Steps to Best Practices* (Topic A-3). Ideally, the committee should be chaired by the administrative judge. It should include a representative of each of the following stakeholders: the primary security provider, such as the county sheriff or chief of police; the clerk of court or court administrator; the district attorney and public defender; other building tenants; first responders; the bar association; county facilities manager; and local elected officials.

Conducting the Initial Committee Meetings

To achieve real progress in making court buildings more secure, members of the security committee must first come together to candidly discuss the security challenges facing them and then agree on how to develop appropriate action plans for moving forward, including funding strategies.

Toward this end, the security committee should convene a meeting involving key internal and external stakeholders for the purpose of: (1) gaining input and discussing the status of court building security and (2) examining possible funding strategies to improve court security. The meeting should have the following objectives:

- To elevate awareness and develop a shared understanding of the nature and scope of risk and the need for improved court building security.
- To develop a basic and shared understanding of the fundamental role that each stakeholder must play in order to publicly support and improve security in an effective and timely manner.
- To design a framework to garner stakeholder input and to work together within an atmosphere of accomplishment and improvement.
- To identify and evaluate the problems that in the past have been barriers to accomplishments and improvements (e.g., funding).

To achieve these objectives, this initial committee meeting will in all likelihood need to be facilitated by an outside, independent party. The facilitator, working in advance with the various key stakeholders, can help elicit their concerns and establish protocols for productive communication in these sessions. After stakeholders' input has been received on what needs to be done cooperatively to improve security in the court building, a briefing report on the meeting needs to be crafted by the committee chairperson and used to guide the court and the committee to implement change and improve security. This briefing document should then be presented to the committee and used as a roadmap to guide all stakeholders interested in improving – or charged with the responsibility for improving – court building security.

Appointment of Task Forces to the Committee

To assist the committee in its efforts to realize positive progress, various task forces, especially one on funding strategies, should be appointed. Examples of other possible task forces include, but are not limited to, such issues as:

- Policies and procedures
- Assignment of security personnel
- Facilities and equipment (e.g., CCTV)
- Building access
- Threat assessment
- Incident reporting

- Contraband analysis
- Training for judges, court staff and officers

The work product of all of the appointed task forces should culminate in a comprehensive and cohesive assessment of what security measures are in place and what additional measures are needed. It is important to note that the *Steps to Best Practices* document, the Appendix to this paper, can serve as a useful guide for assessing what is in place and what is needed. There will no doubt be many improvements that can be achieved without additional resources. Other improvements will require the expenditure of funds from existing or future budget allocations.

It is crucial that all stakeholders on the committee participate in this rigorous needs assessment process so they can be supportive of the resulting plan to improve court building security. This support will include agreeing on what is needed and being part of strategies to secure the additional funding necessary to achieve improved levels of security for the court building.

Funding Strategy

The process for securing additional funding includes fashioning and prioritizing requests arising out of the various task force assessments and recommendations. It also includes stakeholders vigorously advocating for funds from local and state sources. Moreover, other outside sources of funds to improve court building security should be identified and objectively considered, such as accessing funds from private foundations, the Office of Homeland Security, and the Bureau of Justice Assistance. It will be helpful for a coordinator at the state level to serve as a gatekeeper for the process of identifying and pursuing potential outside funding sources.

Developing a Case Statement

Any successful funding strategy will rely on a solid statement that makes a convincing case for what funds are needed and why. A comprehensive, well-structured and documented needs assessment, involving the support of a broad representation of stakeholders, can help to provide the foundation for a solid case statement. The broader the net is cast to involve stakeholders and members of the community, the more allies the court will have in seeking funding.

Further, the needs assessment must lead to a rational, multi-year plan of action as part of the case statement. The action plan should reflect priorities and costs in addressing needs. It is important for stakeholders to realize that not all improvements in court building security require budget requests. As part of the action plan, those security improvements that can be accomplished with little or no money should be identified and swiftly implemented. This initial implementation of security improvements demonstrates to potential funders that the court is serious about security and that it needs additional funds to continue its quest toward achieving best practices in court security.

Those security improvements that do require significant additional funds should be carefully prioritized as part of the multi-year action plan. Part Two of this paper provides a rational basis for prioritizing spending. Such a rational basis can serve to convince funding sources that the court has been careful and thoughtful about its requests.

Other methodologies can be utilized to justify needs. Workload-based staffing models, for example, can be used to support requests for additional security staff in the court building. By analogy, staffing models developed by the NCSC have been successful in justifying the need for additional judges, court staff, district attorneys and public defenders. As these groups have experienced, a needs assessment and development of staffing standards conducted by an outside consultant may lend additional credibility to the funding requests.

Finally, the accountability measures suggested in Part Four of this paper can be helpful in putting together an effective case statement. Funders typically want to know what will be achieved or changed as a result of spending the money requested. As noted in Part Four, it can be challenging to identify what will be accomplished by adding additional security measures or improvements. In essence, a good security program is one that minimizes, or possibly eliminates, incidents by virtue of the security protocols in place. When everything seems to be working and there are no apparent risks, this makes it hard for the court to justify a request for additional funds to improve security. On the other hand, by conducting a security audit of the building and through the use of robust incident reporting and analysis, the court can demonstrate to funders the risks that need to be avoided or mitigated through the use of improved court building security.

Developing a Strategic Funding Plan

Once a convincing case statement is assembled, the security committee needs to develop a strategic plan for securing necessary funds. This is where all stakeholders' participation must be required. To achieve this objective, members of the committee must present a united front for all interested parties. To accomplish a clear assignment of responsibilities and plan of execution well-understood by all, describing who does what and when, is essential.

First, a comprehensive effort must be made to identify all possible sources of funding from various levels of government and other entities. Along with this must come a thorough understanding of the processes entailed in seeking funding from these sources. The largest piece of the funding strategy may be to seek additional funds as part of the court's (or court building tenants') next budget cycle. Another strategy for funding may be to review funds in existing budgets that can be redirected to address crucial security needs.

Second, there should be a clear understanding of who the decision makers are in terms of making funds available for security purposes. Included in this category are legislators, county commissioners, members of the town council, state and local court administrators, as well as other government officials at various levels. The challenge is to effectively convey to these decision makers why court building security is so important, as well as what additional resources are needed in order to achieve a reasonable level of security.

Conveying this message requires careful consideration of two crucial factors: (a) what protocols are involved in talking to decision makers; and (b) who is best suited to convey the message on behalf of the court. It is important that the message be neither oversold nor undersold. It is even more important that the message gets delivered by those, in a united front, who are most likely to have the ear of decision makers.

Every governmental environment has a written or unwritten set of acceptable protocols for discussing resource needs with decisions makers. There are formal avenues such as budget submissions and hearings. There are informal avenues as well, such as topic-based lunches, tours of the court building, or "ride alongs" during court days with

the judge(s).¹ Determining and utilizing the right types and numbers of avenues is critical for success.

Decision makers and their staff are typically bombarded with more information than they can reasonably process. Courts should make sure that messages about court building security are carefully crafted so the essential elements are conveyed in a crisp and cogent manner. Consequences of not funding security requests should be stated in a convincing but not alarmist fashion, although objective examples of tragedies that have occurred at other courts can be used to some extent (e.g., Reno, St. Petersburg, and others).

The final, and perhaps the most important, consideration is the determination of who delivers the message. The most significant factors to consider in selecting messengers are (a) subject matter knowledge, (b) credibility, and (c) relationships. The messengers must first know the subject matter they are presenting. Second they must have a reputation for absolute credibility in order for the message to be well received. Finally, a determination needs to be made as to who among the stakeholders and other interested parties has the best relationship with various decisions makers. Again, decision makers and their staff can be overwhelmed by those wanting their attention. They are most likely to listen to and be receptive of messages from those with whom they have a good personal relationship and can trust.

Overlaying the two factors of protocols and messengers is the absolute need for a unified message. For a funding strategy to be successful, all stakeholders need to present a united front and remain in “lock-step” on messages. Any discord among stakeholders or discrepancy in messages will only serve to confuse decision makers and provide a reason not to fund.

In order to ensure effective execution of the funding strategy, it will be helpful to designate one person, under the auspices of the security committee, to be the primary contact person and coordinator of information and committee members for executing the funding strategy. This one person should have the responsibility to make sure that: (a) the message is well-crafted; (b) the right messengers are using appropriate protocols to

¹ In a “ride along” program, a decision maker, such as a legislator, may spend the day with a judge. This gives the legislator an opportunity to observe first hand a life in the day of a judicial officer.

talk to the right decisions makers; and (c) there is a unified front among all stakeholders at all times.

Conclusion

In an uncertain world, court leaders can be certain of two things: (a) there are inherent and serious risks associated with court building operations, and (b) the level of resources needed to provide a reasonable level of security to protect against these risks will be hard to come by. Given these realities, it is imperative for court leaders to develop and implement effective funding strategies. This is a daunting challenge. The approach outlined in this paper will prove helpful to court leaders as they face this challenge.

Part Four **Accountability and Performance Measures**

Introduction

When budget shortfalls occur in state courts,² difficult *cutback management* decisions are made by municipal, county, and state officials across the country. Funding bodies in most states look closely at performance and accountability of programs when making difficult budget decisions. Court security programs are often targets of these decisions. Therefore, in order to at least maintain the status quo, it is incumbent on courts and the providers of court security programs to be accountable, to document performance, and to objectively prove the worth of court security as an essential function. When demonstrated in courts, accountability more likely than not means there is leadership in place that acknowledges that the measurable productivity of programs is absolutely necessary for continued funding. Continuation and expansion of successful programs in state government happens in those programs that continually measure performance in order to explain, report, and be held accountable for low or non-performance.

The underpinnings that support accountability are the performance, achievement, or accomplishment of a duty or responsibility. In essence, performance can be defined as that which is performed or accomplished, a deed or act which supports the mission of the court and can be measured. In court security programs, this performance is demonstrated not only by the implementation of security policies and procedures, but also by the performance of actions, i.e., protecting the public and employees in a courthouse.

One of the major difficulties with respect to accountability and performance measures in court security programs is that success is difficult to define and to measure. For example, if there are no incidents occurring in the courthouse or in courtrooms, some funding bodies, managers, and employees may contend that they are safe; and they may ask why a lot of money should be spent on court security. Conversely, others, although they may support having security in their court and feel comfortable with its presence,

² According to the Center for Budget and Policy Priorities reported updated December 18, 2009, 43 states have imposed cuts in state spending. On January 3, 2010, according the Associated Press (AP), 36 states are facing severe budget shortfalls in 2010.

often have little understanding or knowledge of how court security works or what it really does to protect them.

For example, not many judges or court employees connect the fact that a court security officer confiscated a person's knife coming into the building with the result that a threat has been reduced. Since the threat of having a knife in the courthouse has been taken away, it is impossible to know whether or not the individual possessing the knife and entering the courthouse would have used it to do harm. Courts and their security providers nationwide are challenged to prove that their security program is effective, that it is necessary for public safety, and that the program needs to continue receiving funding. Courts and their security providers need to be able to prove to their funding bodies that court security is an essential function and should not be cut back. It is analogous to why the Transportation Services Administration (TSA) cannot change its universal screening policy and let people bypass screening stations to board planes unfettered.

The increasing demand for accountability and proof of performance in lean economic times not only puts pressure on courts to develop objectives to prove accountability, but to establish performance measurement systems as well. Courts that want to maintain funding levels for their security programs, in cooperation with their security providers, are now making efforts to build capacity in both areas. Such capacity has traditionally been limited by the lack of objective instruments to evaluate the quality of the security programs and the adequacy of staffing needed to support effective security.

The Need for Data

Funding bodies must have performance measurement data in order to make the correct decisions on the allocation of resources. Objective and unbiased information as to what security measures are being accomplished, what needs additional attention, and what parts of the program are performing at targeted expectation levels, is vital to appropriate resource allocation decisions. Court security programs must compete for funding with other programs in the court, the municipality, the county, or the state. In this day and age, the competition for limited funds is fierce. The collection of data and

subsequent analysis of that data is a must. The following are tools security professionals can use to measure a program's capabilities and effectiveness and, in the long run, to demonstrate the need to continue funds for existing programs and obligate additional funds for expansion.

The Need for Policy and Procedures

In state or municipal courts, most policy statements that provide an umbrella of protection for court employees are written, approved, and promulgated locally or by the state's supreme court. These policy statements often turn into procedures for the establishment and operation of court security programs. A search of the Internet will provide access to numerous state court security handbooks, as well as policies on such wide-ranging subjects as: what is considered contraband in courthouses; cell phone use in courtrooms; who is required to submit to entryway screening; and the membership and range of responsibilities of members of a court's security committee. Such policies and procedures must be subject to performance measures. Not only should these measures be based on the court's mission, vision, goals, and objectives, but the results of the measurement should be linked to the need for resources to properly manage, and if necessary expand, the existing security program.

The Need for Oversight

Oversight of court security programs is necessary to determine accountability and to measure performance. Although oversight usually comes from the managers of court security providers, e.g., the sheriff, it is important to involve all the members on the court security committee – the stakeholders in the system. When committee members become involved in the oversight process, they can regularly monitor policies, procedures, staffing needs, incident reporting, and threat analysis. They can also review response times for such events as building evacuation, hostage-taking, or other emergencies. When all of the parts needed for oversight are in sync, then effective measurement of program performance can more easily occur.

Having oversight in place is also important for the providers of court security to establish measurements and test protocols for assessing their operations and the physical status of their security programs. Hence, the security provider, in cooperation with the

court security committee, can expect consistent application of procedures, testing of performance measures, and accountability.

The Need for Performance Measure

In order to determine and prove success, performance measures of various aspects of the court's security program need to be established. In general there are three types of performance measures: input, output, and outcome. Input measures are tangible and are the basis of the program's components. Such items as budget, staffing, hardware, and the size of the physical plant are not only measurable, but they also relate to certain program goals or objectives. For example, the courts may have as an objective a fully staffed and functional screening station consisting of three court security officers, a magnetometer, and an x-ray machine. This is a best practice guideline that can be adopted as an objective and can be measured. On the other hand, output measures are the products and services produced by the court security programs that can be observed and measured. These measures are what the funding body evaluates when deciding on budget allocation or cutbacks. These are measures that providers, in cooperation with the security committee, can use to prove program effectiveness. Examples of output measures include such items as the number of people screened per day, the amount and types of contraband confiscated, or the number of incidents recorded and successfully responded to. These output measures establish program accountability and provide funders the answers to their questions, such as: "Are we at risk?" "What are you doing to keep us safe?" "What are we getting in return for the money we spend?" "Why shouldn't we reduce your funding request?"

When it comes to protecting people and property, court security programs need to be able to measure such items as the time it takes to evacuate the building and the time it takes to respond to activated courtroom duress alarms or to incidents inside or outside the courthouse. This is achieved through the use of testing – practice evacuations and practice responses to duress alarms. The use of testing and the collection of resulting data is what can fundamentally defend security programs. Equipment must be tested to make sure duress alarms are active, that CCTV cameras work, that magnetometers are properly calibrated, that contraband is collected and incidents are being analyzed, that

courtroom and personal safety training is provided for judges and court staff, that court security officers are adept at reading x-ray machines, that intrusion alarms are monitored after hours, and that the courthouse is protected after hours from intruders. Testing should occur regularly and randomly (test weapons through magnetometers), but the testing process used must follow established protocols. Identifying, establishing, testing, and proving the effectiveness of output measures is at the heart of program success. Without them, court security programs that cannot prove their essential functions are at the mercy of the ebb and flow of good and bad funding times.

The Need for Outcome Measures

Outcome measures represent the impact the court security program has on public and employee safety. In essence, the measurement of outcomes proves the occurrence or non-occurrence of an undesired situation. For example, if a gunman is killed trying to shoot his way into a courthouse by court security officers at entryway screening (St. Petersburg, Florida, May 7, 2008) is the court security program successful? When a man enters a federal courthouse (Las Vegas, Nevada, January 4, 2010), kills a court security officer, injures a United States Marshal, does not make his way past screening and into the courthouse to harm others, and is ultimately shot and killed across the street from the courthouse, did entryway screening work? The vast majority of people will answer these questions with a resounding, “Yes, thankfully!”

Outcome measures are used to assess how well individual tasks are performed in relationship to overall program goals. These measures can support various program objectives. The regular audit or assessment of court facilities and the monitoring of subsequent improvements made is one way to reduce risk. For example, reducing public entrances to the courthouse from several to one by implementing the steps to best practice guidelines contained in the Appendix, supports the goal of improving public and employee safety. Or when measuring emergency preparedness, it is important to determine as an outcome measure how often table top exercises or practice evacuations drills are conducted. This event can be measured by how participants behave during the exercise or how evacuees react during the drill. Do they assume their role and correctly react during the exercise? Do they leave the building(s) in a timely fashion and assemble

at the correct location? Do all judges and jurors comply with the drill? Another outcome measure should involve cost. In relation to cost, the following questions should be answered: Are court security officers (CSOs) being reduced or expanded over time? Why? Are volunteer court security officers being trained and used in the program to reduce costs? Do judges and court staff receive regular safety training? Is the presence of a uniformed CSO directly related to the reduction of incidents?

The Need to Implement Performance Measures

Using performance measures to substantiate accountability is useful for all decision makers involved in the operation and success of the court security program. For example, performance measures can be used to determine whether the program is supporting the strategic direction of its funders. Performance measures may be used in many other ways by: (1) demonstrating effectiveness to program managers and court security committee members; (2) assessing emergency preparedness capabilities; (3) evaluating and maintaining equipment; and, most important, (4) determining the adequacy of resources to support operational and legal requirements necessary to measure court security program success. Physical (security) related performance measures provide valuable information that not only can be used to support funding requests or to accomplish program objectives, but also to identify areas for improvement and to increase public and employee safety. It is important to note that physical performance measures are always more tangible, and in a sense easier to measure, than process items such as program support and attitude.

The Need for Incident and Threat Reporting

In order for accountability and performance measures to be effective and credible, they must be supported by a comprehensive and robust incident and threat reporting system. All incidents and threats within a court building must be promptly reported. Those observing incidents or receiving threats must be aware of how to report and to whom to report. All reports of incidents and threats must be reviewed at an appropriate level and action taken by responsible parties as warranted. Information contained in incident and threat reports, to include actions taken in response, should be analyzed and catalogued on an ongoing basis. This information can provide a solid foundation for

performance and accountability measures by identifying in a systemic way the security challenges a court faces and the resources required to meet those challenges.

Conclusion

The proof of accountability through the use of performance measures can be instrumental as an integral component of an effective case statement for funders, as described in Part Three. Those making decisions on funding typically want to know what will be achieved or changed as a result of spending the money requested. In essence, they want to know what the problem was and how the work of the program resulted in a solution.

For court security programs in eras of budget reductions, proving accountability through use of performance measures is the most important way to demonstrate to funding bodies that the provision of security hardware and staffing is working and that as a result their investment in the security program is working. Objective determination of the success of input, output, and outcome measures not only will document the effectiveness of providing public safety to funding bodies, but it will also provide security providers and court leadership a management tool as well as a basis for documentation of future needs. Finally, using performance measures to establish accountability will ensure consistency of operations and cost-effective program management, improve the overall management and protection of court facilities, and ensure the safety of employees and the public at-large.³

³ Portions of this part of the report on Accountability and Performance Measures are extracted from an article entitled *Use of Physical Security Performance Measures* by the Department of Homeland Security.

Appendix

Steps to Best Practices



STEPS TO BEST PRACTICES FOR COURT BUILDING SECURITY

JANUARY 2010

**Timothy F. Fautsko
Steven Berson
James O'Neil
Kevin Sheehan**

**Daniel J. Hall, Vice President
Court Consulting Services
707 Seventeenth Street, Suite 2900
Denver, Colorado 80202-3429**

Introduction

The National Center for State Courts (NCSC), through its Court Consulting Division, has conducted security assessments of court buildings as well as personal security and safety training throughout the country. In conducting court building assessments, the NCSC assessment team has evaluated court security in terms of “best practices” – guidelines describing those security measures that should be in place with respect to a comprehensive set of topics covering court buildings and court operations. These best practices are not only based on the considerable experience of NCSC assessment team members, but are also a compilation of various guidelines from the U.S. Marshals Service, National Sheriffs’ Association, International Association of Chiefs of Police, the Transportation Safety Administration, the Department of Homeland Security, and the National Association for Court Management. The NCSC assessment team recommends that leadership in every court building strive to achieve best practices in all topic areas to provide a suitable level of security for all those who work in or visit the court building.

Acknowledging that implementing best practices in court building security will require increasingly scarce budgetary resources, the NCSC assessment team has also developed steps in phases that can be taken toward achieving best practices in various areas of court building security. These steps may be a useful approach to courts as they strive to implement improvements in court building security. The NCSC assessment team wishes to emphasize that a fully effective integrated level of security will be reached only when all the measures at the best practices level are incorporated. The NCSC assessment team has provided these steps in phases, so that a court at its discretion can adopt incremental improvements before reaching the level of best practices. These steps in phases are plateaus along an ascending path to improvement – improvement the NCSC assessment team recommends that courts achieve over time.

It is important to note that *Steps to Best Practices* focuses almost exclusively on security matters. With rare exception, issues of emergency preparedness, continuity of operations, and disaster recovery are not within the scope of this document.

Security is not a one-time achievement. It is a serious and continuous goal and requires constant vigilance. Further, it must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and they can never be eliminated. But with proper attention and care, they can be minimized. Paying close attention to the recommendations contained in *Steps to Best Practices* will help courts minimize the risks.

Steps to Best Practices is organized by steps, phases, topics, and categories. It will be helpful for the reader at the outset to have a working understanding of each of these terms:

- Steps: These are specific buildings blocks, specific actions that courts can take to improve security.
- Phases: These are logical groupings of steps forming a temporary plateau in terms of security measures in place.
- Topics: These are the subject areas into which steps in phases are organized.
- Categories: These are sets of topics. There are four categories listed in priority order. (*Note: Topics within each category are listed in alphabetical rather than priority order.*)
 - Category A. These are fundamental topics that must be addressed first in order to provide a base on which to place all of the others.
 - Category B: These are topics that are extremely important to address.
 - Category C: These are topics that are very important to address.
 - Category D: These are topics that are important to address.

CATEGORIES AND TOPICS

Topic

Category A: Fundamental

One	Command and control center
Two	Policies and procedures
Three	Security committee

Category B: Extremely Important

One	Access of people into court building
Two	After-hours access to court building
Three	Chambers
Four	Courtrooms
Five	Court security officer (CSO) staffing levels
Six	Duress alarms
Seven	Threat and incident reporting
Eight	In-custody defendants
Nine	Training

Category C: Very Important

One	Closed circuit television (CCTV)
Two	Emergency equipment and procedures
Three	Interior access during business hours (circulation zones)
Four	Intrusion alarms
Five	Jurors
Six	Parking (particularly for judges)
Seven	Public counters and offices

Category D: Important

One	Cash handling
Two	Exterior/interior patrols
Three	Perimeter issues
Four	Public lobbies, hallways, stairwells, and elevators
Five	Screening mail and packages

Category A: Fundamental

These three topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices*.

- **Command and control center.** Without such a center, the necessary and vital technological tools for court building security – closed circuit televisions (CCTV*), duress alarms, and intrusions alarms – cannot be utilized or monitored in an effective manner.
- **Policies and procedures.** Without these, there is no way to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices* to inform the process of developing a comprehensive and cohesive set of policies and procedures.
- **Security committee.** Without such a committee, meeting regularly and empowered to exercise rigorous oversight on all matters relating to security within the court building, it is difficult, if not impossible, to properly assess and address the myriad of security challenges facing court leadership.

**CCTV, as used in this document, refers to a variety of old and new technologies. For detail, see topic C-1.*

TOPIC A-1: COMMAND AND CONTROL CENTER

Phase One

1. Establish a command and control center in the lobby area of the court building with an assigned court security officer (CSO)*. For smaller court buildings, the monitoring function of a command and control center can take place at the front entrance screening station.
2. Provide for telephone/radio communication as a point of contact between a CSO and potentially vulnerable areas of the court building, such as courtrooms.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Design and construct a command and control center that is isolated from the main lobby of the court building.
4. Design a control panel that will provide space for administrative activity and equipment to monitor CCTV cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and radio dispatches.

**Note: CSO is defined as an individual trained in court security and certified to use a firearm. The CSO should also be armed with a triple-retention holster and a radio that can communicate with the command and control center. The CSO at the command and control center does not necessarily need to be armed.*

Best Practice

Continue all steps in Phase One and Two, plus add the following:

5. Install control panels and monitoring equipment for CCTV surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch.
6. Provide additional security personnel as required to supervise and monitor command and control center activities.

TOPIC A-2: POLICIES AND PROCEDURES

Phase One

1. Judicial branch leadership understands the need for and commits to the implementation of effective, comprehensive security based on best practice models and establishes orders directing court security policies and procedures.

Phase Two

Continue with the step in Phase One, plus add the following:

2. Establish a task force under the direction of the court security committee (see Topic A-3) and with the cooperation of the appropriate law enforcement agency(s), to draft essential documents for the establishment of the policies and procedures on court building security. The task force on policies and procedures should include:
 - Court administration
 - Security personnel
 - Facilities management
 - Fire and rescue personnel
 - Others responsible for and impacted by court security
3. Create the package of essential documents to include:
 - Policies and procedures to include:
 - Overall court security operations
 - Screening protocols
 - Define contraband that cannot be brought into the court building and confiscate it at the door.
 - Procedures to govern courtrooms and other areas in the event of a security incident
 - Risk and resource assessment instruments and protocols for use
 - Incident reporting instruments and protocols for use

- Operations manuals and materials
- Training manuals and materials
- Administrative orders with authority to revise

Phase Three

Continue all steps in Phases One and Two, plus add the following:

4. Establish communication to stakeholders that allows for feedback and adjustments as follows:
 - Assign a liaison between task force and stakeholders.
 - Provide periodic briefings in various formats to stakeholders.
 - Solicit formal feedback from stakeholders.
 - Adjust package (e.g., policies, procedures, manuals, materials) as necessary.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

5. Provide training and evaluate the package as follows:
 - Train everyone with a direct role in court security.
 - Conduct drills to test procedures.
 - Evaluate results of the drills.
 - Evaluate results of response to actual incidents.
 - Modify the package to improve practice.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

6. Review and update policies and procedures at least every other year.
7. Analyze Phases Two through Four for operational effectiveness.

TOPIC A-3: SECURITY COMMITTEE

Phase One

1. Establish a court security committee at the court building, which is chaired by a judge (preferably presiding) and has a membership of at least the primary security provider, such as the sheriff or CSO, the clerk of court, and the court administrator.
2. The judge or court administrator should meet regularly with law enforcement officials to discuss security concerns and improve security at the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Add the district attorney and public defender or representative from the state bar to the court security committee.
4. Add tenants as members of the security committee as appropriate.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Add elected officials to the court security committee.
6. Add an ad hoc member to the court security committee to serve on a task force for the committee.
7. Undertake a self-assessment of the security in place within the court building. Checklists with which to conduct these assessments are available from various sources, such as the National Sheriff's Association. Assistance in conducting assessments is also available from the NCSC.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Establish an integrated court security committee and use task forces to provide the committee with additional research and information gathering capacity. Additional members added to the committee or on task forces should include:
 - Court staff members working in the court building
 - Local and state government officials
 - Local and state subject matter experts
9. Reconstitute the court security committee to be additionally responsible for emergency preparedness, disaster recovery/continuity of operations plan (COOP), and response to pandemic flu, and add members with this expertise as appropriate. Rename the committee the court security and emergency preparedness committee.
10. Add planning responsibility for building new or improving current court facilities to the newly named committee.

Category B: Extremely Important

TOPIC B-1: ACCESS OF PEOPLE INTO COURT BUILDING

Phase One

1. Establish only one main door through which the public can enter the court building and display a sign at the entrance clearly listing those items that cannot be brought into the court building.
 - Designate one or more of the doors to the building to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through public entrances.
 - Keep all other exterior doors locked during business hours.
 - Emergency exit bars should be installed on all external exit doors. All exit doors should be alarmed, with ten second delay consistent with local codes. Establish signage that explains the “Exit Only” requirement.
2. Establish protocols for entry through locked doors.
 - Tailgating* or bringing in family members/friends through these doors should not be allowed.
 - Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.

**Note: In this context, tailgating is when an individual(s) enters a court building with a person who is authorized to properly gain entry with an access card or key.*
3. Assign one CSO to guard the public entrance to the court building on a full-time basis.
4. Set up a table or other physical structure at the public entrance to serve as a screening station.
5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
 - Provide screener with a weapons ID chart.
 - Provide screener with a list of contraband items.
6. Train the CSO for all Phase One tasks described above.
7. Provide basic court security orientation training for judges and staff.

Phase Two

Continue all steps in Phase One, plus add the following:

8. Add a magnetometer at the main door (public entrance) to the court building.

9. Conduct a daily calibration and inspection of magnetometer, preferably by an authorized and trained supervisor.
10. Train CSO(s) in all tasks added in Phase Two, plus provide additional security training for judges, staff, jurors, and others.
11. Replace keys to the court building with access cards for judges, authorized court staff, and other building tenants' staff.
12. Install a CCTV camera at main door (public entrance) to the court building.
13. Assign a second CSO* to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
14. Establish a code notification procedure between law enforcement and the court so screeners are aware if a dangerous person is likely to enter the building.
15. Add a duress alarm at the screening station.
16. Establish a policy that law enforcement officers entering the building on personal business may not bring in a weapon.

**Note: Staffing level in Phase Two is one full-time CSO at the screening station, plus one additional CSO for high-volume times.*

Phase Three

Continue all steps in Phases One and Two, plus add the following:

17. Install an x-ray machine at the public entrance screening station.
18. The second CSO referenced in step 13 should be assigned as a full-time, permanent CSO* to operate the public screening station. During slow periods, this second CSO can still be available for additional duties as described in step 13.
19. Establish additional policies and procedures for Phase Three operations as follows:
 - Conduct an annual inspection and certification of x-ray machines.
 - Provide detailed, step-by-step manual and training on screening procedures.
20. Train CSOs in all tasks and provide security orientation training for judges and staff.
21. Add a CCTV camera at the judge/staff entrance door.

**Note: Staffing level in Phase Three is two full-time CSOs at the screening station.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

22. Assign a third CSO* to operate the public screening station: one CSO to operate the magnetometer, one to operate the x-ray machine, and one to handle problems. During low traffic times, the third CSO can assume another assignment. Ideally,

- all three CSOs should be armed, but at least one should be armed. (Armed CSOs should use a triple-retention holster.)
23. If two or more public screening stations are in operation, assign a fourth CSO as a supervisor to oversee operations.
 24. Install a magnetometer, x-ray machine, duress alarm, and CCTV camera to the judge/staff entrance. Consider allowing jurors to use this entrance.
 25. Assign at least two CSOs to the judges/staff entrance if staff or jurors use this entrance and at peak hours during the day. Otherwise, assign at least one CSO.
 26. Establish a universal screening policy. Universal screening means everyone entering the building is screened
 27. When everything is in place, establish a policy that only law enforcement officers with responsibility for court security inside the building may bring a weapon into the building. Other law enforcement officers should be required to check their weapons in a lock box at the screening station(s).

**Note: Staffing level in Best Practice is three full-time CSOs for each public screening station, plus one additional CSO to supervise multiple stations, and two CSOs assigned to judge/staff/juror entrance.*

TOPIC B-2: AFTER-HOURS ACCESS TO COURT BUILDING

Phase One

1. Permit access into all areas of the court building via key or electronic card access. Keys and cards should be issued and controlled pursuant to a comprehensive accountability system that has been approved by the court's security committee.
2. Conduct background checks prior to issuing a key or access card to any person.
3. Conduct background checks for cleaning crews and any vendors granted after-hours access to the building. Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court.
4. Monitor the activities of the public while in the building after hours.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Eliminate the use of keys and implement the use of an access card system. As necessary, issue keys to a limited number of people only for emergencies, building maintenance purposes, and building security responsibilities.
6. Create a single access point into the court building that is guarded by a CSO who checks IDs and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
7. Update background checks periodically (at least annually).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

8. Conduct a full screening requiring everyone to go through the magnetometer and x-ray station.

TOPIC B-3: CHAMBERS

Phase One

1. Install a duress alarm at the judge's desk and in the chamber's reception area.
2. Test duress alarms regularly – at least monthly.
3. Provide training to judges regarding personal security and safety in chambers.
4. Escort judges when leaving a chambers area for a courtroom if chambers hall is unsecured.
5. Keep existing chambers window coverings adjusted so activities cannot be observed from outside the court building
6. Conduct daily sweeps of chambers in the morning and at the end of the day.
7. Keep entrance doors to chambers area locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Assign at least one CSO or transport deputy to be present whenever an in-custody defendant is escorted through chambers hallway.

Phase Two

Continue all steps in Phase One, plus add the following:

9. Install vertical blinds as interior window coverings in all chambers.
10. Install duress alarms in conference room(s).
11. Plan for and conduct drills regarding emergency situations in chambers area.
12. Escort judges when leaving secure chambers and courtroom area.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

13. Assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallway, with one to clear the path ahead. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
14. Install ballistic-resistant material in all accessible windows (e.g., ground level, first floor). The recommended ballistic-resistant material should meet UL Standard 752, Level IV, unless a lower level can be justified by an assessment of the risks based on such factors as adjacent structures and geographic features associated

with the location of chambers. This level may be reduced based on specific security assessments.

15. Request cleaning crews to clean chambers at the end of the day when court staff is present, rather than at night.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

16. Install CCTV cameras in chambers hallways that lead to the entrance to chambers areas.
17. If feasible given the existing structure of the court building, establish a secure path for judges to go from chambers to courtroom (no escorting of in-custody defendants). If feasible, establish a secure path to escort in-custody defendants from holding cells to the courtroom without going through chambers hallways.
18. Install ballistic-resistant material in all chambers windows that are located on floors above ground level.
19. Prohibit cleaning crews from entering chambers unsupervised at any time. Require cleaning during the day or leave waste baskets outside locked chambers area doors at night. The judge or court staff should be present when cleaning crews are physically cleaning/dusting chambers during the day.

TOPIC B-4: COURTROOMS

Phase One

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a “rover” from one courtroom to the next (unless local or state rules require additional coverage). There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.
2. Install duress alarms in the courtroom at accessible locations:
 - On top or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk’s stationTrain judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)
5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.

6. Install and then regularly test emergency lighting/fire equipment in courtrooms.
7. Always keep front and back doors to courtrooms locked when courtroom is not in use.
8. Use proper and acceptable restraints per state law on in-custody defendants.
9. Prohibit use of camera/cell phones in the courtroom and prohibit other items that could be used as weapons.

Phase Two

Continue all steps in Phase One, plus add the following:

10. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in a courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present.
11. Install one CCTV camera in criminal and family courtrooms.
 - The camera should be installed in the back of the courtroom in order to monitor activities in the courtroom up to and including the well and bench area.
12. Holding cells in the courtroom should be properly constructed and escape-proof.
13. Every three or four months, debrief incidents that have occurred in the courtrooms and review procedures related to courtroom security. This de-briefing should take place in the courtroom. There should be an immediate debriefing on any serious security incident.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

14. A second CSO should be assigned to a courtroom whenever any court proceeding is being held. Whether or not there is an in-custody defendant, one CSO should be assigned for the judge and one for the courtroom. A second CSO is not ordinarily needed for civil cases, unless specifically requested by a judge based on a determination of a higher risk involved in a particular case.
15. Install one CCTV camera in all remaining courtrooms.
 - The camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
16. Install two CCTV cameras in criminal and family courtrooms.
 - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.
17. Begin the process necessary to establish a courtroom in the jail for advisements/arraignments and other hearings. Use video arraignment* originating from the jail for in-custody hearings as much as permitted by state law.

**Note: Video arraignment is the preferred solution to bringing in-custody defendants back and forth for settings and brief hearings.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

18. For high-visibility trials, an additional CSO should be assigned to be present in the courtroom.
19. Use video or a courtroom in the detention center for all arraignments or hearings to set dates of next appearance.*
**Note: Use of video is the preferred solution to personal appearance by in-custody defendants whenever legally feasible by state law.*
20. Conduct sweeps of all courtrooms, including the random use of trained dogs.
21. Provide separate working offices (not in the courtroom) for clerks and others to use after courtroom proceedings have been completed.
22. Use bullet-resistant materials when constructing or retrofitting the bench and workstations inside the courtroom. The most recent recommended standard for these materials is UL Standard 752 Level III.
23. Install two CCTV cameras in all courtrooms.
 - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.

TOPIC B-5: COURT SECURITY OFFICER (CSO) STAFFING LEVELS

Phase One

1. One CSO* should be permanently assigned to the main entrance of the court building during business hours.
2. One CSO or transport deputy should be assigned to the courtroom while there is an in-custody defendant in the courtroom.
3. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a rover from one courtroom to the next. There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.

**Note: It is estimated that each CSO post requires approximately 1.33 full-time employees to cover for sick and annual vacation, training, etc.*

Phase Two

Continue all steps in Phase One, plus add the following:

4. As additional CSOs become available, assign in the following priority per recommended phases leading up to Best Practices in each relevant topic:
 - To meet recommended staffing guidelines at screening station (see Topic B-1)

- To meet recommended staffing guidelines for the courtroom (see Topic B-4)
- To meet recommended ratios for transporting in-custody defendants (see Topic B-8)
- To assign patrols for the interior and exterior of the building (see Topic D-2)

Best Practice

Continue all steps in Phase One and Two, plus add the following:

5. Achieve full recommended staffing guidelines for the following topics:
 - Screening stations (see Topic B-1)
 - Courtrooms (see Topic B-4)
 - Transporting in-custody defendants (see Topic B-8)
 - Regular patrols of building interior and exterior (see Topic D-2)

TOPIC B-6: DURESS ALARMS

Phase One

1. Install duress alarms in the courtroom and at the bench, clerk's station, and CSO station. Training should be provided on the functionality of duress alarms and on the protocols for use.

Phase Two

Continue step in Phase One, plus add the following:

2. Install alarms in each chamber and reception area.
3. Install alarms at public counters, cash areas, and other offices where the public has access, including those without counters.
4. Install alarms in the interview and mediation rooms.
5. Install alarms and 911 contact ability at the childcare center, if the court building includes such a center.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. Install alarms at screening stations.
7. Install an alarm in the jury assembly room.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install duress alarms in the holding cell area.
9. Install a duress alarm in the loading dock area.
10. Install a duress alarm in the mailroom.

TOPIC B-7: THREAT AND INCIDENT REPORTING

Phase One

1. Establish a policy requiring incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible. The more serious the incident, the more quickly it should be reported.
2. Train CSOs and staff in the court building on how to define what an incident is and how to report incidents verbally and in writing.
3. Develop and use an incident reporting form and submit forms in writing to the proper authorities, at least on a monthly basis.

Best Practice

Continue all steps in Phase One, plus add the following:

4. Implement a practice for periodically evaluating incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court security committee (and the committee's incident reporting task force).
5. Provide general feedback to staff on incidents, particularly to those who reported them (e.g., complete the feedback loop).

TOPIC B-8: IN-CUSTODY DEFENDANTS

Phase One

1. Assign at least one CSO or transport deputy to escort in-custody defendant(s) through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO or transport deputy to remain with defendant(s) in courtroom at all times.
3. Efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum.
4. When transporting in-custody defendant(s) in public hallways, bystanders should be moved to one side of the hall. When transporting in-custody defendant(s) in a public elevator, the elevator should be cleared of all other people.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
6. Make sure all holding cells and areas within the court building are appropriately structured, secured, staffed, and searched daily.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Install CCTV cameras along entire in-custody defendants' escort route.
8. Establish a secure sally port for in-custody defendants entering the building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

9. Establish a secure pathway for a defendant from the transport bus, through the sally port, to the holding cell and the courtroom to avoid crossing the path of judges, staff, or public.

TOPIC B-9: TRAINING

Phase One

1. CSOs should be trained in court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, and safety and weapons certification.
2. New judges and court staff should receive an initial court security orientation briefing that includes emergency procedures, building evacuation routes, building emergency color codes system, and personal safety procedures for work and home.
3. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

4. All CSOs should receive at least 16 hours of mandatory in-service training on court security each year.

5. Establish a judge and staff security education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and at home.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. In addition to annual qualification with firearms, establish mandatory refresher court security training programs for CSOs, to include such topics as emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage, shooter-in-place, and judicial protection.
7. Establish mandatory, ongoing security and safety education programs for judges and court staff that include such topics as handling difficult people, home safety techniques, safety practices for inside and outside the court building, hostage incidents, and emergency evacuation from the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. In addition to annual qualification with firearms, establish annual mandatory refresher court security training programs for CSOs to include first-aid, defensive tactics, handcuffing, courtroom security, and judicial protection.
9. Establish mandatory ongoing security and safety education programs for judges and court staff that include handling difficult people, high-profile trials, home safety techniques, safety practices inside and outside the court building, hostage incidents, travel safety tips, threats, and emergency evacuation from the court building.
10. Train judges and court staff in self-defense and techniques for hostage-taking situations.

Category C: Very Important

TOPIC C-1: Closed Circuit Television (CCTV)

Phase One

1. Install a digital and color CCTV camera system* at the entry screening station and in the courtroom(s) facing the gallery.

**Note: CCTV systems can utilize varying kinds of technology to transmit video images and to provide for system access and control. Cables have been the traditional means of system connectivity. Newer technologies have emerged over time. Some systems now utilize an internet protocol (IP) to transmit data and control signals over a fast Ethernet link. Another technology, virtual local area network (VLAN), allows authorized personnel to access cameras or a recorder from a remote setting. Courts are encouraged to explore and adopt the technologies that best suit their needs and budgets.*

CCTV cameras should have the following functional capacity:

- Fixed or pan, tilt, zoom. These types of CCTV cameras are typically used by most courts. Fixed cameras with a wide-angle lens allow for a stationary focus on areas of interest. The capacity to tilt and pan allows each camera to maximize its area of coverage, thereby minimizing blind spots and the number of cameras needed. The ability to zoom allows each camera to capture a more accurate and close-up picture of what is actually transpiring in a particular scene.
- Color. This is standard in current systems. Black-and-white images cannot tell the full story. Important features are indistinguishable. Only with a color monitor can faces and other specific objects be clearly identified.
- Recording capacity. The CCTV system should have digital video recording capacity enabling a CSO to view incidences at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation issues. The operation and recording function of a camera can be set to activate by either motion or sound, or by the setting off of duress or intrusion alarms.
- Signs. Notices should be conspicuously placed to inform the public that CCTV cameras are operating and recording activity in the area.

Phase Two

Continue the step in Phase One, plus add the following:

2. Install CCTV cameras in detention areas to monitor activities in holding cells.
3. Install CCTV cameras on building perimeters and secure parking lots.

4. Install CCTV cameras to monitor activity at public counters and in offices where the public may visit.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Install CCTV cameras at the loading dock.
6. Install CCTV cameras in hallways.
7. Install CCTV cameras in each courtroom.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install CCTV cameras in elevators and stairwells.
9. Install CCTV cameras at screening stations.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

10. Install CCTV cameras in hallways that access chambers.
11. Install CCTV cameras in the mailroom.
12. Install CCTV cameras in the childcare area, if such an area exists.
13. Install CCTV cameras to cover all pathways through which an in-custody defendant may be escorted.
14. Install CCTV cameras to cover the interior areas of all doors to the court building and to all accessible windows.

TOPIC: C-2 EMERGENCY EQUIPMENT AND PROCEDURES

Phase One

1. Use emergency color codes to designate emergency procedures for evacuation. An example of such a code system is attached as part of the Appendix.
2. Have an emergency, battery-generated lighting system in courtrooms, offices, and public areas.
3. Have a fire extinguisher on each floor, with egress floor plans posted.
4. Have fire alarms placed on each floor.
5. Have an elevator(s) that meets state and local fire codes, i.e., MGM fire code.

Phase Two

Continue all steps in Phase One, plus add the following:

6. Have an emergency generator system that is properly fenced-in and protected.
7. Test generator system monthly; keep a log of tests.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Have CCTV cameras installed in the elevator(s).
9. Have automated external defibrillators (AEDs) located accessibly on each floor and designate a person(s) in the court building who is trained to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
10. Designate a floor warden on each floor to ensure proper response to emergency codes.
11. Have an enunciator fire alarm and extinguisher system.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

12. Have a floor warden identified and trained on each floor to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
13. Designate a safe area for a command and control center during an emergency.
14. Consider advising judges and staff by public address system, bull horn, email, or phone. One method of warning is the use of Court Building Warning Codes; a sample can be found in the Appendix.
15. Have an evacuation plan that everyone in the court building has been familiarized with.
16. Have a bomb-threat protocol and a lockdown plan in place.

TOPIC C-3: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES)

Phase One

1. Establish the concept of circulation zones (separate areas and routes) for the following:
 - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, back of public counters, private elevators, secure stairways)
 - In-custody defendant transport (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms)

- Public (e.g., restrict the public to public zones)
2. All doors that are required to be locked, in accordance with the court buildings circulation zone concept, should be kept locked at all times. Such doors should never be left propped open.
 3. Have a key or access card system to control access based on a system approved by the administrative authority of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience. This system should:
 - Be under the control of a central authority
 - Require background checks for all card or key holders
 - Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination)

Phase Two

Continue all steps in Phase One, plus add the following:

4. Eliminate keys and require access cards. Maintenance staff and emergency responders should retain keys.
5. Establish viewing ports (peepholes) to prevent non-authorized access through secured courtroom doors.
6. Improve definition and enforcement of circulation zones.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Establish some form of video recognition (phone) system to allow access into secure areas.
8. Continue to improve definition and enforcement of circulation zones.
9. Install a CCTV camera system in all secure areas in the court building to monitor activity.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Establish and maintain maximum separation among zones (e.g., In-custody defendants are not escorted through secure hallways; judges do not pass through public areas when going to and from their cars, through screening, and to and from chamber areas.)

TOPIC C-4: INTRUSION ALARMS

Phase One

1. All exterior doors should have basic intrusion alarm devices, covering:
 - All locked doors after hours.
 - Emergency exit doors during business hours.

Phase Two

Continue the step in Phase One, plus add the following:

2. Install intrusion devices on all accessible windows, either glass-break or motion detector.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

3. Establish a fully integrated intrusion system with the following functionalities:
 - When a court building is closed, every external door should be equipped with a device that will trigger an alarm at the control center of the appropriate responding agency and identify the intruded area.
 - During business hours, every door that is kept locked should be equipped with a device that will trigger an alarm that will identify the area intruded at the command and control center within the building. Every locked door with an emergency exit bar should trigger an alarm whenever anyone uses it, with a ten-second delay consistent with local codes
 - When the building is closed, this alarm should go to the control center of the appropriate responding law enforcement agency; when the building is open, the alarm should go to the building's command and control center.
 - All windows that are reasonably accessible from the exterior perimeter of the building (e.g., first floor, basement, possibly second floor) should be protected against intrusion. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

4. Integrate CCTV cameras into the system described above so that cameras will be activated in the area(s) of intrusion.

TOPIC C-5: JURORS

Phase One

1. Provide jurors with court security information before they report for duty by placing information on the jury summons they receive. For example:
 - Where to enter the court building
 - What items (e.g., knives, nail files, scissors) should not be brought into the court building
 - Not to discuss cases with anyone before and during jury service
 - Not to wear juror ID badges outside the court building
2. Screen jurors as they enter the court building or before they report to the jury assembly area.
3. Give a basic security and building evacuation orientation and ID badge to jurors at the assembly area before going to the courtroom. Cover such matters as what to do in case of an emergency and how to respond to a coded emergency announcement.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Assign a CSO to the jury room whenever juror payment is being made and when juror funds are obtained and transported back and forth to the court building.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

5. Assign a CSO to provide security inside and outside the jury assembly room when jurors are present.
6. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervise the loading of jurors and another CSO should meet the jurors on the floor on which they disembark.
7. Assign a CSO to remain with the jury during the entire trial/deliberation.

**TOPIC C-6: PARKING
(PARTICULARLY FOR JUDGES)**

Phase One

1. Remove all signs in judges' parking area that identify spots either by name or title of judge. Any signs should simply say reserved along with a number as appropriate.
2. Each judge should notify law enforcement officials or a CSO of their arrival in the morning and be escorted into the court building if they park in an unprotected public parking lot.
3. Judges should be escorted to the unprotected parking lot by a CSO when they leave at night.

Phase Two

Continue the steps in Phase One, plus add the following:

4. Fence in the judges' parking lot and require that an electronic card access system is used for entrance into the court building. Install privacy slats if a chain-link fence is used.
5. Judges and court staff should be escorted to their cars or other mode of transportation after business hours.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

6. Provide secure parking for judges, court staff, and jurors.
7. Install CCTV cameras in secure parking lots.
8. Provide judges and court staff a regular patrol presence in the parking areas in the morning, during the lunch hour, and at close of business.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

9. Provide a secure parking area, preferably covered, for judges where they can proceed directly from their car, through screening, to their chambers without traversing any public areas or main court building entrance areas.

TOPIC C-7: PUBLIC COUNTERS AND OFFICES

Phase One

1. Install one or more duress alarms at the main public counter. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in offices (e.g., drapes, blinds) lowered to restrict observation from outside.
3. Install Plexiglas-type enclosures at cash counters.
4. Keep cash and checks in a secure, locked area overnight.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Install Plexiglas-type enclosures at all public counters.
6. Install duress alarms strategically in the back areas of offices.
7. Keep cash and checks and daily change locked in a safe overnight.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Install CCTV cameras at all public counters.
9. Install an alarm on the safe.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Install CCTV cameras overlooking the safe.
11. Provide regular security patrols by CSOs at the public counters.

Category D: Important

TOPIC D-1: CASH HANDLING

Phase One

1. Develop and train court staff on procedures for handling cash. The procedures should:
 - Determine who should collect the money.
 - Determine how to safeguard money during the daytime work hours and overnight.
 - Train staff on how to verify checks and reconcile fees.
 - Determine industry standards for deposits.
2. Install protective barriers and duress alarms at cash counters.
3. Use an office safe for money storage.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Install CCTV cameras at counters and in the office.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Use an armored car service or the bank's personnel to pick up funds daily.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require two people – one court staff and an armed CSO – when carrying cash.

TOPIC D-2: EXTERIOR/INTERIOR PATROLS

Phase One

1. Request that the local law enforcement agency conduct exterior patrols, particularly during times when the building is closed.
2. Develop a memorandum of understanding (MOU) with local law enforcement regarding which agency is responsible to protect the exterior of the court building during and after business hours.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Conduct regular CSO interior patrols by CSOs assigned to work in the court building, focusing on crowded hallways.
4. Assign CSO exterior patrols both regularly and randomly throughout the day.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Continue to increase both interior and exterior CSO patrols of the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require scheduled patrols of all interior and exterior areas 24/7, either by CSOs or local law enforcement officers.

TOPIC D-3: PERIMETER ISSUES

Phase One

1. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness. It should also be sufficient for perimeter CCTV cameras to capture images.
2. Keep doors locked after hours and allow access only via appropriately authorized key or access cards.
3. Keep all shrubbery and trees properly trimmed to prevent hiding places or access to the court building roof for persons or packages.
4. Conduct daily security checks around the perimeter.

Phase Two

Continue steps in Phase One, plus add the following:

5. Provide a secure parking area for judges with signs that do not indicate that the space is being used by a judge (e.g., signs should not say for official use only).
6. Install intrusion alarms to cover all exterior doors and accessible windows.

Phase Three

Continue steps in Phases One and Two, plus add the following:

7. Install CCTV cameras around the perimeter (at each corner of the court building).
8. Install bollards as necessary outside selected (main) entrance doors, ground floor (accessible) windows, and other vulnerable areas.
9. Enclose and secure all exposed utilities.

Best Practice

Continue steps in Phases One, Two, and Three, plus add the following:

10. Replace keys with an electronic card access system (except for back-up emergency) on exterior door entrances to the court building.
11. Provide secure parking for staff and jurors. Secure parking for judges and staff should have the following attributes:
 - Protected from public access
 - Protected from public view
 - Required electronic access, by way of card or other appropriate device
 - CCTV cameras in place and operating

TOPIC D-4: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

Phase One

1. Provide emergency lighting in the court building.
2. Establish egress/ingress standards regarding stairwells, hallways, and elevators.
3. Establish emergency evacuation procedure and evacuation diagrams.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Designate secure and public elevators.
 - Provide secure elevator(s) for judges.
 - Provide secure elevator for prisoner transport.
5. Install appropriate signage to alert the public to what items cannot be brought into the court building (i.e., guns, knives, scissors).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Install CCTV cameras in lobbies, hallways, stairwells, and elevators in the court building and provide secure elevator(s) with electronic card access.
7. Assign a CSO to regularly patrol these areas in accordance with an assigned schedule.
8. Install a public address system in the building to facilitate announcements and emergency codes.

TOPIC D-5: SCREENING MAIL AND PACKAGES

Phase One

1. Provide routine visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items.
2. Require staff to attend training on postal security and package identification techniques provided by the United States Postal Service (USPS).
3. Develop and practice a response protocol with law enforcement when a package is identified as suspicious or dangerous.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Require all mail and packages to be processed through an x-ray machine.
5. Require everyone delivering mail or packages to pass through the magnetometer.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Best practice is to establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:
 - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious) upon being received at the mailroom. This includes all USPS mail delivered and picked up by court staff from the local post office.

- Deliveries of flowers, candy, food, gifts, etc., to any person located in a court building should be cleared through the mailroom first, be verified and vouched for by the recipient, screened as appropriate, and then delivered.
- Mailroom staff should sort incoming mail and packages off site by building, division, and/or department and prepare them for acceptance by designated representatives of each court office or division.
- Designated representatives of each court office or division should go to the mailroom, pick up mail for distribution to their offices, and identify questionable items. All authorized court and other staff mail handlers should attend training on handling suspicious mail. Local USPS or postal inspectors may conduct advanced training for state and local government agencies.

Sample Court Building Color Codes

Professional emergency responders advise that, as much as possible, communication during an emergency should be clear, understandable, and simple. Presently, state and local courts use different warning systems and language to advise court building occupants what to do during an emergency. The decision whether to stay or leave a court building during an emergency often can be the difference between life and death.

Realizing that clear communication and understandable instructions are vital, courts have been advised by the NCSC to use universal color codes and practice drills to augment their existing evacuation procedures. Using the same color-coded language in every court building will ensure that employees will understand and react properly to emergencies.

- **Code Yellow – Situational Awareness**
 - Cautionary: Be aware and prepared to react to danger.
 - A dangerous situation may be developing in the court building.

- **Code Red – Imminent Danger**
 - Stay put! An active shooter is in the court building or there is a hostage situation.
 - Get into an emergency protective posture or in a safe haven.

- **Code Green – Emergency – Evacuate Building**
 - Listen to instructions from your floor warden.
 - Report to your assigned location away from court building.

- **Code Blue – Emergency Team Responding**
 - An emergency team is responding to or is in the court building.
 - Wait for further instructions from officials.

- **Code White – Administrative/Informational**
 - Return to normal operations.
 - All is well.



STEPS TO BEST PRACTICES *for*
COURT BUILDING SECURITY

Nathan W. Hall
Steven V. Berson
Timothy F. Fautsko
James F. O'Neil
Kevin W. Sheehan
Hon. V. Lee Sinclair, Jr.



Daniel J. Hall, Vice President
Court Consulting Services
707 Seventeenth Street, Suite 2900
Denver, Colorado 80202-3429

ACKNOWLEDGEMENTS

The development and publication of this revised report has been made possible by the support and hard work of many people. The National Center for State Courts (NCSC) wishes to acknowledge the developers of this document, Nathan Hall, Senior Court Management Consultant at the NCSC and security consultants Steven Berson, Timothy Fautsko, James O’Neil, Kevin Sheehan, and Judge Lee Sinclair. The NCSC also extends its appreciation to the members of the Conference of Chief Justices/Conference of State Court Administrators Security and Emergency Preparedness Committee and their staffs for carefully reviewing this document and making important recommendations that have improved the final product. Finally, the NCSC extends thanks to its editorial staff, Darcy Hitt and Zana Molina, for the many hours they spent providing quality assurance in the conformation and final editing of the original and revised publications.

Published February 2010. Revised January 2013. Revised September 2016.

Copyright © 2016 National Center for State Courts. All rights reserved.

TABLE OF CONTENTS

INTRODUCTION	1
CATEGORY A: FUNDAMENTAL	3
TOPIC A-1: SECURITY COMMITTEE	4
TOPIC A-2: POLICIES AND PROCEDURES.....	5
TOPIC A-3: THREAT AND INCIDENT REPORTING.....	9
TOPIC A-4: SECURITY TRAINING.....	10
CATEGORY B: CRITICAL	12
TOPIC B-1: COMMAND CENTER.....	12
TOPIC B-2: IN-CUSTODY DEFENDANTS	13
TOPIC B-3: COURTROOMS	14
TOPIC B-4: CHAMBERS.....	17
TOPIC B-5: ACCESS OF PEOPLE INTO COURT BUILDING	19
TOPIC B-6: PUBLIC SERVICE AREAS, COUNTERS, AND OFFICES.....	23
TOPIC B-7: JUDGES PARKING	25
TOPIC B-8: PERIMETER ISSUES.....	26
CATEGORY C: ESSENTIAL	28
TOPIC C-1: AFTER-HOURS ACCESS TO COURT BUILDING	28
TOPIC C-2: EMERGENCY EQUIPMENT.....	29
TOPIC C-3: INTRUSION DETECTION SYSTEMS.....	29
TOPIC C-4: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES).....	31
TOPIC C-5: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS.....	32
TOPIC C-6: JUROR SECURITY AND CIRCULATION.....	33
TOPIC C-7: CASH HANDLING	34
TOPIC C-8: SCREENING MAIL AND PACKAGES	35
STAFFING, DURESS ALARM, AND SECURITY CAMERA RECOMMENDATIONS INCLUDED IN THE BEST PRACTICES	37
COURT SECURITY OFFICER (CSO) STAFFING LEVELS	37
DURESS ALARMS.....	38
SECURITY CAMERAS.....	38
CONCLUSION	40

INTRODUCTION

The National Center for State Courts (NCSC), through its Court Consulting Services division, has conducted security assessments of court buildings as well as personal security and safety training throughout the country. In conducting court building assessments, the NCSC has evaluated court security in terms of “best practices” – guidelines describing those security measures that should be in place with respect to a comprehensive set of topics covering court buildings and court operations. These best practices are not only based on the considerable experience of NCSC security experts, but are also a compilation of various guidelines from the United States Marshals Service, National Sheriffs’ Association, Conference of Chief Justices/Conference of State Court Administrators Joint Committee on Court Security and Emergency Preparedness, International Association of Chiefs of Police, Transportation Safety Administration, the Department of Homeland Security, and the National Association for Court Management. The NCSC recommends that leadership in every court building strive to achieve best practices in all topic areas to provide a suitable level of security for all those who work in or visit the court building.

Implementing some of the best practices in court building security may be a challenge in view of constrained or otherwise limited budgetary resources. Accordingly, best practices are set forth in a format of steps and phases, an incremental approach that envisions an effective level of security upon implementation of all measures. These steps may be a useful approach to courts as they strive to implement improvements in court building security. The NCSC wishes to emphasize that an effective level of security will be reached when all the measures at the best practices level are incorporated. The NCSC has provided these steps in phases, so that a court at its discretion can adopt incremental improvements before reaching the level of best practices. These steps in phases are plateaus along an ascending path to improvement – improvement the NCSC recommends that courts achieve over time.

It is important to note that *Steps to Best Practices for Court Building Security* focuses almost exclusively on security matters. With rare exception, issues of emergency preparedness, continuity of operations, and disaster recovery are not within the scope of this document.

Steps to Best Practices for Court Building Security is organized by steps, phases, topics, and categories. It will be helpful for the reader at the outset to have a working understanding of each of these terms:

TERMS USED IN STEPS TO BEST PACTICES

- Steps: These are specific buildings blocks and/or specific actions that courts can take to improve security.
- Phases: These are logical groupings of steps forming a temporary plateau in terms of security measures in place.
- Topics: These are the subject areas into which steps in phases are organized.
- Categories: These are sets of topics. There are three categories listed in priority order, with Category A taking top priority.
 - Category A: These are fundamental topics that should be addressed first in order to provide a base on which to place all of the other topics.
 - Category B: These are critical topics to be addressed after the Category A topics.
 - Category C: These are essential topics to be addressed after the Category A and B topics.

CATEGORY A: FUNDAMENTAL

The four topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices for Court Building Security*:

- **A-1: Security Committee.** A court building security committee, meeting regularly and empowered to exercise oversight and sustain matters related to security within the court building, is a prerequisite to enable the court and its stakeholders to properly assess and address the myriad of security challenges facing court and stakeholder leadership.
- **A-2: Policies and Procedures.** A cohesive and comprehensive set of security policies and procedures is necessary to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices for Court Building Security* to further the process of developing a meaningful and effective set of policies and procedures.
- **A-3: Threat and Incident Reporting.** Threat and incident reporting is of paramount importance to the safety of judges, court employees, and the public who visit the court building. Enacting a threat and incident reporting system enables stakeholders to review and develop responses to potential negative events and reinforces security best practices.
- **A-4: Security Training.** Every single person who works in a court building has the potential to materially enhance the safety and security of his or her work environment, to be the “eyes and ears” of a workforce constantly alert to risks and threats. Judges and court staff that have been well trained on well-publicized policies and procedures provide the best means for this eyes and ears function to be effectively discharged.

TOPIC A-1: SECURITY COMMITTEE

PHASE ONE

1. Establish a court building security committee for the court building, to be chaired by a judge (preferably presiding) and having membership of at least the primary security provider and a representative of the county or other funding source.
 2. The court building security committee should operate its meetings on an action planning process of “who does what, by when, and what resources are needed.” The committee should initially meet monthly to discuss and implement recommendations contained in this report. Then, it should meet at least quarterly to discuss and propose solutions to other security problems.
 3. The judge or court administrator should meet with court security personnel and law enforcement officials on a regular basis and after any negative event to discuss security concerns and improve security at the court building.
-

PHASE TWO

Continue all steps in Phase One, plus add the following:

4. Add security committee members representing all “stakeholders” who have an interest in security at the court building. Stakeholders, by way of example, include county facilities management, the district attorney and public defender, the state or local bar, the probation department, and other non-court tenants of the court building. In terms of the size of the committee, a balance should be struck between inclusivity of stakeholders and the need to keep the committee at a manageable size. (Stakeholders not represented on the committee can be appointed to task forces per Step 6 below.)
-

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

5. Undertake a self-assessment of the security in place within the court building. Checklists with which to conduct these assessments are available from various sources, such as the National Sheriff’s Association. Assistance in conducting assessments is also available from the NCSC.
-

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Form task forces to provide the committee with additional research and information gathering capacity. For example, an “Incident Reporting and Contraband” task force could be chaired by a member of the security committee and be responsible to set up an incident reporting and contraband analysis system that not only collects data, but actively analyzes it, reports on actions taken, and presents recommendations for change to the committee. Additional members added to various task forces could include:
 - Court staff members working in the court building, including IT staff
 - Local and state government officials
 - Local and state subject matter experts
7. Add security-based planning responsibility under the committee for court facility design, construction, and renovation projects.
8. Periodically engage an independent professional organization to conduct an audit of security measures in place for the exterior and interior of the court building.

TOPIC A-2: POLICIES AND PROCEDURES

PHASE ONE

1. Under the auspices of the court building security committee (see Topic A-1) the leadership of the court, county (or other funding body), and law enforcement should understand the need for and commit to the development and implementation of effective and comprehensive court building security policies and procedures. It is important to note that judges are particularly at the forefront of court building security. Judicial leadership is crucial in the development and implementation of security policies and procedures.

PHASE TWO

Continue the step in Phase One, plus add the following:

2. Establish a task force under the direction of the court building security committee, and with the cooperation of the appropriate law enforcement agency(s), to draft a cohesive and comprehensive set of court building security materials, to include such items as policies and procedures, operations manuals, training manuals, contingency plans, and incident reporting and risk assessment instruments and protocols. Subject matters to be covered by this comprehensive set of materials include by way of example:
 - Screening operations and protocols, including the definition of weapons and illegal items/contraband prohibited from the court building. This should also include confiscation, seizure, and removal processes for such instances.

- Management of “negative events” such as:
 - Bomb threat
 - Suspicious package
 - Fire
 - Medical emergencies
 - Violence in the courtroom or elsewhere in the court building
 - Escapes by in-custody defendants
 - Active shooter
 - Severe weather/power outage
- Management of high-visibility trials.
- Prohibiting the use of cameras/cell phones in the courtroom and prohibiting other items that could be used as weapons.
- Defining the roles of Court Security Officers (CSOs) and those responsible for court security in the building.
- Defining who has authority to bring weapons into the court building.
- Developing an emergency management manual, to include, for example, such matters as:
 - Lockdown and evacuation procedures for judges’ chambers and courtrooms, and for all other areas of the court building.
 - Designating a floor warden on each floor to ensure proper response to emergency instructions.
 - Designating a floor warden identified and trained on each floor to respond to medical emergencies (e.g., cardio pulmonary resuscitation (CPR) and use of an automated external defibrillator (AED)), while 911 is called.
 - Designating a safe area for staff to assemble and remain in place during an emergency or negative event.
 - Designating a safe area for a command center during an emergency or negative event.
 - Developing methods for notifying judges and employees of emergencies or negative events, including the use of Communication Warning Codes (see below).
 - Developing evacuation plans that everyone in the court building has been familiarized with.
- Defining specific security policies and procedures for sequestered juries.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

3. Establish communication with employees of all stakeholders that allows for feedback and revision of security materials as follows:
 - Assign a liaison between task forces and stakeholders.
 - Provide periodic briefings in various formats to stakeholders.
 - Solicit formal feedback from stakeholders.
 - Revise court building security materials as necessary based on stakeholder feedback.
4. Officially adopt the court building security materials. Issue appropriate court orders on key security matters. To be successful, security documents need the support of judges. Court orders give legitimacy and enforceability to security policies. Examples of key matters warranting a court order include subjecting visitors to screening and ordering staff to be screened as well.
5. Publish the court building security materials. The level of detail and the audience to whom materials are published should be determined on a need to know basis.

PHASE FOUR

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Practice and evaluate the court building security materials as follows:
 - Conduct drills and exercises to test policies and procedures.
 - Evaluate the results of the drills.
 - Evaluate the results of responses to actual negative events and incidents.
 - Revise the court building security materials as warranted based on an evaluation of the results of drills and actual incidents.
7. Invite first responders and SWAT units to walk the court building and grounds with CSOs to familiarize the first responders with the facilities and request that the SWAT unit utilize the court building for training on a periodic basis.

BEST PRACTICE

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

8. Review and update policies and procedures on a bi-annual basis and after major incidents, events, and facility renovation projects.
9. Analyze Phases Two, Three, and Four for operational effectiveness.

COMMUNICATION WARNING CODES FOR COURT BUILDINGS

The NCSC, as well as professional emergency responders, suggest that communication during an emergency be clear, understandable, and simple. Presently, state and local courts use many different warning systems and language to advise court building occupants what to do during an emergency which can be confusing.

As a result of the shootings at Columbine High School in Colorado, color codes were originally developed by a high school administrator in Olathe, Kansas. Since that time, color codes followed by verbal commands have been widely used in schools, in colleges and universities, in hospitals, and in federal and state courts to quickly direct employees what to do when an emergency occurs. The decision whether to stay or leave a court building during an emergency can often be the difference between life and death.

Realizing that clear communication and understandable, simple instructions are vital in any building emergency, courts use color codes, verbal commands, and practice drills to augment their existing evacuation procedures. Using the same color codes followed by verbal instruction in every court building will ensure that court employees can assist other building tenants, jurors, and the public how to react properly to emergencies.

RECOMMENDED COLOR CODES

- **Code Red** – **Imminent Danger**
 - An active shooter is in the court building or there is a hostage situation.
 - Get into an emergency protective posture or in a safe haven per the predetermined emergency response plan (e.g., run, hide, fight).
- **Code Orange** – **Emergency: Evacuate Building**
 - Listen to instructions from your floor warden.
 - Report to your assigned location away from the court building.
- **Code Yellow** – **Emergency: Team Responding**
 - An emergency team is responding to or is in the court building.
 - Wait for further instructions from officials.
- **Code Blue** – **Situational Awareness**
 - Cautionary: Be aware and prepared to react to danger.
 - A dangerous situation may be developing in the court building.
- **Code Green** – **Administrative/Informational**
 - Return to normal operations.
 - All is well.

TOPIC A-3: THREAT AND INCIDENT REPORTING

DEFINITIONS¹

THREAT – is a statement of an intention to inflict pain, injury, damage, or other hostile action on someone (court employee or court attendee) or an institution (court building) in retribution for something done or not done now or in the future. A threat is synonymous with a threatening remark, warning, or ultimatum such as a menace to a person or institution. A threat can be a person or a thing likely to cause damage or danger.

INCIDENT – is an action or communication that causes or threatens to cause personal injury, property damage, or disrupts courthouse proceedings. Courthouse proceedings include activities in the courtroom and outside the courtroom and within the facility, e.g. chambers, clerk’s offices, etc. Note: This definition is focused on the potential that an action may manifest physically (personal injury, property damage) or be a threat of the same.

PHASE ONE

1. Establish a policy requiring threats and incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible, but no later than the close of business on the day in which a threat or incident occurred. The more serious the threat or incident, the more quickly it should be reported.
 2. Train CSOs, judges, and staff in the court building on how to recognize threats and incidents and how to report them orally and in writing.
 3. Develop and use threat and incident reporting forms and submit forms in writing to the proper authorities, at least on a monthly basis, preferably in electronic format so the designated reporters can more easily file their reports, and necessary guidance/assistance can be provided more readily. The court building security committee should receive a copy of all threat and incident reports.
 4. Coordinate threat and incident information with interested parties at the state and county level. Establish a “feedback loop” that travels in all directions.
-

BEST PRACTICE

Continue all steps in Phase One, plus add the following:

¹ Source: Implementation Plan: Courthouse Security Pilot, US. Bureau of Justice Assistance, December 18, 2009.

5. Implement a practice for regularly evaluating incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court building security committee (and the committee's incident reporting task force).
6. Provide general feedback to staff on incidents, particularly to those who reported them (e.g., complete the feedback loop).
7. Establish an electronic system for reporting threats and incidents, to enable quick review and deployment of resources, and to enable multiple shareholders to have near-instant opportunities to review and respond. A database should be maintained on all pertinent information, to include organizational responses and any follow-up activities. Databases should be maintained at the local and state level.

TOPIC A-4: SECURITY TRAINING

PHASE ONE

1. Acknowledge that training is the glue that binds all court building security measures together. Security training needs to be frequent, repetitive and simple. Without training, staff and CSOs will never be prepared for the unexpected. Every staff member and CSO needs security training. It is essential that training be mandatory and universal. Judges in particular need to participate. Nothing gets staff to buy in to security more than a judge actively participating in security training. The judge sets the tone.
2. New judges and court staff should receive an initial court security orientation briefing that includes such topics as shooter in place and hostage-taking, emergency procedures (e.g., for fire, weather and medical emergencies), building evacuation routes, building emergency color code system, and personal safety procedures for work and home.
3. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.
4. CSOs should be trained in basic court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, threat de-escalation techniques and safety and weapons certification.
5. CSOs should receive basic training in emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage situations, active-shooters, and judicial protection.
6. Command center staff should be trained in critical incident command and crisis communications.

PHASE TWO

Continue all steps in Phase One, plus add the following:

7. Establish a judge and staff security continuing education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and off-site.
8. All CSOs should receive at least 24 hours of mandatory in-service training on court security each year.
9. Invite first responders, particularly the SWAT team, to do a walk-through of the court building. Encourage the SWAT team to utilize the court building as part of their own training program.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

10. Establish mandatory, ongoing security and safety education programs for judges and court staff that include topics addressed in the initial security orientation briefing, along with such topics as handling difficult people, anger-management, home safety techniques, safety practices for inside and outside the court building, hostage incidents, and emergency evacuation from the court building.
11. In addition to annual familiarization and qualification courses on firearms and intermediate weapons, establish regularly scheduled mandatory advanced refresher training courses for CSOs, to include such topics as emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage situations, active-shooters, and judicial protection.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

12. Establish mandatory ongoing security and safety education programs for judges and court staff that include high-profile trials, home safety techniques, travel safety tips, suspicious packages, bomb and other threats, and emergency evacuation from the court building.
13. Train judges and court staff on self-defense options, threat de-escalation techniques, and personal safety/security considerations during hostage situations.
14. Establish and schedule advanced court security training programs for CSOs to include threat de-escalation, security assessments, judicial protection, incident response, dangerous individuals, mental health issues, and high threat proceedings.

CATEGORY B: CRITICAL

TOPIC B-1: COMMAND CENTER

PHASE ONE

1. Establish a command center² in a central, secure, strategically located area of the court building with an assigned court security officer (CSO*). In smaller facilities where limited resources are available, a command center may consist simply of a monitor at a CSO's desk or workstation. The CSO assigned to the command center is not necessarily required to carry a firearm. For smaller court buildings, the monitoring function of a command center can take place close to the front entrance screening station.
2. Alarms should be constantly monitored at the command center.
3. Provide for telephone/radio communication as a point of contact between a CSO and potentially vulnerable areas of the court building, such as courtrooms and chambers.

**Note: A CSO, as referenced throughout this document, is defined as an individual trained and qualified in court building security, and has been specifically trained and qualified to use a firearm and intermediate weapons, e.g., Taser, chemical spray, or restraints (i.e. handcuffs, leg restraints). Additional CSO information can be found under the CSO Staffing Levels topic below at p. 37.*

PHASE TWO

Continue all steps in Phase One, plus add the following:

4. Construct a command center in a secure area located within the court building. If this is not feasible, make sure that there is closely-restricted access to the command center, and that there is ballistic-resistant protection over the command center's doors, windows, and other areas subject to attack.

² A security command center, as referenced in this document, refers to a physical location where all security activities for the court building are controlled and all security infrastructure is monitored. A security 'command center' has a different function than an in-custody defendant 'control room' which is used to manage the transport and housing of in-custody defendants. In some court buildings, the command center and control room are combined into a single facility as a way to gain building and staffing efficiencies.

5. Install control panels and monitoring equipment for security surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch.

BEST PRACTICE

Continue all steps in Phases One and Two, plus add the following:

6. Provide additional security personnel as required to supervise and monitor command center activities. The command center should be staffed at all times when the court building is open to the public.
7. The individuals staffing a command center should not be the physical responders to a crisis. Removing them from the command center to the “fight” would result in the loss of a critical element providing situational awareness to emergency responders and staff. The situational awareness provided by the command center allows responders to make the best tactical decisions and staff to decide whether to shelter in place or run.

TOPIC B-2: IN-CUSTODY DEFENDANTS

PHASE ONE

1. Assign at least one CSO or transport deputy to escort in-custody defendants through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO to remain with defendants in the courtroom at all times.
3. In courthouses lacking a secure in-custody defendant circulation, efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum. The public should be cleared to the side of hallways and other areas prior to the escort of in-custody defendants.
4. When escorting in-custody defendants in public hallways, bystanders should be moved to the far end of the hall; not to one side or the other. When escorting in-custody defendants in a public elevator, the elevator should be cleared of all other people.
5. In-custody defendants should be properly restrained while being escorted, using handcuffs, ankle restraints, and belly chains. (They should not be handcuffed from the front.)
6. In-custody defendants should have no contact of any type, physical or verbal, with the public, family, or friends while being escorted or while in court.

PHASE TWO

Continue all steps in Phase One, plus add the following:

7. Establish a control center to manage the transport and housing of in-custody defendants. The control center should include monitoring capacity and control of all doors and elevators within the secure in-custody defendant circulation area. As stated in the previous section, in some courthouses, this function may be located and managed together with the building security command center.
8. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the in-custody defendant should be armed with an intermediate weapon, e.g., Taser or chemical spray; the other officer trailing behind should be armed.
9. Make sure all holding cells and areas within the court building are appropriately structured, secured, staffed, and searched before and after each occupation.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

10. Install security cameras along the entire in-custody defendants' escort route.
11. Establish a secure sally port for in-custody defendants entering the building

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

12. Establish secure circulation for a defendant from the transport bus, through the sally port, to the holding cell and the courtroom to avoid crossing the path of judges, staff, or the public.

TOPIC B-3: COURTROOMS

PHASE ONE

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a "rover" from one courtroom to the next (unless local or state rules require additional coverage).
2. There must be at least one CSO present throughout the entire court proceeding whenever an in-custody defendant is involved.

3. Install duress alarms in the courtroom at accessible locations:
 - On top or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk's station
4. Train judges and staff on the functionality of duress alarms and on the protocols for use.
5. Test duress alarms regularly (at least monthly).
6. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. Note: In any phase, for high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband. In addition, courtrooms should be cleared and locked during a recess or when the courtroom is otherwise not in use. If individuals are allowed to stay in the courtroom during a recess, a CSO should be assigned to remain in the area.
7. Secure or remove items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers. Secure or remove all moveable furniture (e.g. moveable or folding chairs). (Such chairs can be secured by fastening them together with plastic ties around their legs.)
8. Install and then regularly test emergency lighting/fire equipment in courtrooms.
9. Always keep front and back doors to courtrooms locked when the courtroom is not in use. It should be possible to easily lock all courtroom doors from the inside.
10. The courtroom door nearest the bench should be kept closed but unlocked while court is in session to allow easy and unfettered egress for the judge at the bench. This assumes that a CSO will be present in the courtroom to prevent any unauthorized attempts to access the chambers area while court is in session. If the presence of a CSO cannot be ensured, a crash bar should be installed along with a card reader override. If a card reader is installed, it will be important to make sure judges keep their access cards handy and in close possession while in court.
11. Use proper and acceptable restraints per state law and a judge's approval on in-custody defendants. In-custody defendants, except during a jury trial or as prohibited by law, should be restrained with handcuffs, leg restraints, and belly chains.
12. Install door scopes (i.e. peepholes) for the judge's entry into the courtroom.
13. Ensure weapons as exhibits are rendered inoperable. Ammunition should always be secured in sealed evidence bags separate from any firearms.
14. Issue orders of decorum for the courtroom.
15. For high-visibility trials, and for other proceedings as warranted, institute other security measures such as leaving the front row of the gallery vacant and/or separate family and friends of the plaintiff or prosecution from family and friends of the defendant.

16. Develop policies to keep defendants seated during pleas and sentencing hearings. A seated defendant is more easily controlled and less likely to be disruptive.
17. Keep presentation tables and podiums a safe distance away from the bench.

PHASE TWO

Continue all steps in Phase One, plus add the following:

18. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in the courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present. The transport officer maintaining custody (i.e., having direct contact) of the in-custody defendant should be armed with an intermediate weapon (e.g., Taser, stun gun, or chemical spray, etc.) in lieu of a firearm. This will minimize the likelihood of an in-custody defendant obtaining a firearm during confrontations.
19. Install **one** security camera in criminal and family courtrooms. The primary security camera should be installed in the back of the bench facing the gallery. (Refer to later phases for installation of an additional camera.)
20. Holding cells for the courtroom should be properly constructed, safe for the in-custody defendants, and escape-proof.
21. Every three months, a judge should convene a meeting with court staff to debrief on incidents that have occurred in the courtroom and to review procedures related to courtroom security. There should be an immediate debriefing following any significant security incident.
22. Install bullet-resistant materials at the bench and workstations inside courtrooms. Opaque ballistic-resistant material that meets UL Standard 752, Level III, should be installed behind the vertical surfaces on the three sides of the benches and stations that are visible to the public. Bullet-resistant fiberglass panels are a cost effective material that can be field cut or factory cut to specific dimensions and installed on the backside of existing courtroom millwork.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

23. A second CSO should be assigned to a courtroom whenever any court proceeding is being held. Whether or not there is an in-custody defendant, one CSO should be assigned for the judge and one for the courtroom. A second CSO is not ordinarily needed for civil

cases, unless specifically requested by a judge based on a determination of a higher risk involved in a particular case.

24. Install one security camera in all remaining courtrooms. The camera should be installed in the back of the bench facing the gallery.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

25. For high-visibility trials, an additional CSO should be assigned to be present in the courtroom.
26. Establish a courtroom in the jail for advisements/arraignments and other hearings. Use video arraignment originating from the jail for in-custody hearings as much as permitted by state law. Video arraignment is the preferred solution to bringing in-custody defendants back and forth for settings and brief hearings.
27. Conduct sweeps of all courtrooms, including the random use of trained dogs.
28. Provide separate working offices (not in the courtroom) for clerks and others to use after courtroom proceedings have been completed.
29. Install two security cameras in all courtrooms:
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom as described in a previous step.
 - A second camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
30. Install an automatic electronic lock-down mechanism for the courtroom.

TOPIC B-4: CHAMBERS

PHASE ONE

1. Provide training to judges and court staff regarding personal security and safety in chambers.
2. Install a duress alarm at the judge's desk and in the chamber's reception area.
3. Test duress alarms regularly – at least monthly. Train judges and court staff in how and when to use the duress alarms in chambers.
4. Escort judges when leaving a chambers area for a courtroom if the chambers hall is unsecured.
5. Keep existing chambers window coverings adjusted at all times so that activities cannot be observed from outside the court building.
6. Conduct daily sweeps of chambers in the morning and at the end of the day.

7. Keep entrance doors to chambers area locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Provide advance notice to judges so they do not step outside their chambers while in-custody defendants are being escorted in the hallway.
9. Position furniture in chambers with security in mind. For example, the judge's access to the exit door should not be blocked by a visitor's chair. Also, the judge's chair should be positioned if at all possible to avoid a direct line of sight from the outside.

PHASE TWO

Continue all steps in Phase One, plus add the following:

10. Install blinds, preferably vertical, as interior window coverings in all chambers.
11. Keep blinds positioned at all times so as to prevent a view into chambers from the outside.
12. Establish a video intercom and remote controlled magnetic door strike system to control access into chambers areas.
13. Plan for and conduct drills regarding emergency situations in chambers areas.
14. Have CSOs escort judges when leaving secure chambers and courtroom areas.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

15. In locations where there are no dedicated transportation corridors for in-custody defendants, assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallways, with one to clear the path ahead. The transport officer assigned direct contact with the in-custody defendant should not carry a gun, but be armed with an intermediate weapon such as a Taser or chemical spray; the other officer should carry a firearm in a triple retention holster.
16. Install a sound and light (e.g., strobe) system in the hallways by chambers to alert judges and staff when in-custody defendants are about to be escorted through the hallway.
17. Install ballistic-resistant material in all accessible windows (e.g., ground level, first floor). The recommended ballistic-resistant material should meet UL Standard 752, Level IV, unless a lower level can be justified by an assessment of the risks based on such factors as adjacent structures and geographic features associated with the location of chambers. This level may be reduced based on specific security assessments.
18. Request that cleaning crews clean chambers at the end of the day when court staff is present, rather than at night. Cleaning crews should be supervised by someone who is accountable to the court.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

19. Install security cameras in chambers hallways that lead to the entrance to chambers areas.
20. If feasible given the existing structure of the court building, establish a secure path for judges to go from chambers to courtrooms (no escorting of in-custody defendants). If feasible, establish a secure path to escort in-custody defendants from holding cells to the courtroom without going through chambers hallways.
21. Install ballistic-resistant material in all chambers windows that are located on floors above ground level.
22. Install duress alarms in conference room(s).
23. Cleaning crews should be prohibited from entering judges' chambers unsupervised at any time. Require cleaning during the day or leave waste baskets outside locked chambers area doors at night. The judge or court staff should be present when cleaning crews are physically cleaning/dusting chambers areas during the day.

TOPIC B-5: ACCESS OF PEOPLE INTO COURT BUILDINGS

PHASE ONE

1. Establish only one main entrance through which the public can enter the court building. Post signage at the main entrance that states all persons are subject to search by security. This signage should also include a listing of those items that are not allowed to be brought into the building.
 - Keep all other exterior doors locked during all hours, including business hours.
 - Emergency exit bars should be installed on all exterior exit doors. All exit doors should be alarmed, with a ten second delay consistent with local codes. Alarms should sound at the command center. Establish signage that explains the "Exit Only" requirement. (Avoid panic bar alarms with a "local alarm" feature in favor of an alarm that sounds in the command and control center.)
 - Conduct a security "sweep" of the court building in the morning before the building is open to the public and each evening after all areas of the building are closed to the public.
2. Establish protocol for entry (i.e. controlled access) through secured doors.
 - Designate one of the doors to the building (preferably staffed by an armed and qualified CSO) to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors

should not be permitted to use this door but should enter through the public entrance.

- Policies and procedures need to be developed and enforced on prohibiting staff from bringing in others (such as co-workers, family members, and friends) through secure doors. “Tailgating” through secured doors should never be allowed. In this context, tailgating is when an individual(s) enters a court building following a person who is authorized to properly gain entry with an access card or key.
3. Dedicate a full-time CSO position to secure the main public entrance to the court building.
 4. Until a screening station design can be constructed, set up a temporary table and other physical structures (e.g. stanchion ropes, dividers, etc.) to serve as the screening station. Ensure that sight lines from the screening station and the building entrance/exit are unobstructed to allow for appropriate visual assessment and security response.
 5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
 - Provide screener with ability to contact the command center by way of a radio.
 - Provide screener with a weapons identification chart.
 - Provide screener with a list of contraband items.
 - Provide screener with a listing of daily court activities.
 - Provide screener with a list of phone numbers for judges, bailiffs, and other court staff.
 6. Train CSOs in all Phase One tasks.
 7. Provide basic court security orientation training for judges and staff.
 8. Each court building should have access to at least one magnetometer that can be made available for use in high-visibility trials or other special circumstances.

PHASE TWO

Continue all steps in Phase One, plus add the following:

9. Install a magnetometer at the main door (public entrance) to the court building.
10. Per system manufacturer specifications, conduct a daily testing and inspection of the magnetometer. Recalibrate the magnetometer as necessary. This should be conducted by an individual who has received the required training.
11. Train CSO(s) in all tasks added in Phase Two, plus provide additional security training for judges, staff, jurors, and others.
12. Replace keys to the court building with access cards for judges, authorized court staff, and other building tenants’ staff. Assignment of access cards must be restricted to an “as required” basis as determined under the purview of the court building security

committee. When keys are utilized, make sure they are double-cut, non-duplicate keys. Develop an inventory list for all cards and keys. When anyone's employment is terminated, cards should be deactivated and keys turned in on the last day that the card or key holder is present in the court building.

13. Install a security camera at the main door (public entrance) to the court building.
14. Install a security camera at any separate entrance(s) for judges, court employees, or attorneys.
15. Install a security camera over each locked exterior door, along with two-way audio capability.
16. Assign a second CSO* or contract security officer to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
17. Establish a direct line of communication between law enforcement and the courts so screening personnel are aware of potentially dangerous individuals who may seek to enter the court building.
18. Add a duress alarm, telephone, and gun lockers at the screening station.
19. Establish a policy that only law enforcement officers with responsibility for court security, or are inside the building in an official capacity, may bring a weapon into the building. Officers entering the court building on personal business (including uniformed and plain clothes officers) may not bring in a weapon and should be required to check their weapons in a lock box at a secure location adjacent to the screening station(s). Officers that are in plain clothes on official business must wear visible identification while in the court building if they are carrying a concealed weapon.

**Note: Staffing level in Phase Two is one full-time CSO at the screening station, plus one additional CSO or contract security officer for high-volume times.*

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

20. Install an x-ray imaging system at the public entrance screening station.
21. The second CSO or contract security officer referenced in step 16 should be assigned as a full-time, permanent CSO* or contract security officer to operate the public screening station. During slow periods, this second CSO or contract security officer can still be available for additional duties as described in Task 16 above.
22. Train CSOs and contract security officers in all tasks and provide security orientation training for judges and staff.

23. Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. Delivery people and packages should be screened through a magnetometer and x-ray machine respectively. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.
24. Provide screening staff with ballistic-resistant vests and require staff to wear vests at all times.
25. Install ballistic-resistant shields to protect screening staff.
26. Establish additional policies and procedures for Phase Three operations as follows:
 - Conduct an annual inspection and certification of x-ray imaging system. This equipment must be registered with state health and safety agencies.
 - Provide a detailed, step-by-step manual, training, and continuing education on contemporary screening procedures.

**Note: Staffing level in Phase Three is two full-time security officers at the screening station, at least one of whom is a CSO.*

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

27. Assign a CSO* as the third security officer to staff the public screening station: one to operate the magnetometer, one to operate the x-ray imaging system, and one to handle problems. During low traffic times, the third CSO can assume another assignment. Ideally, all CSOs should be armed, but at a minimum, one should be armed. (Armed CSOs should be outfitted with triple-retention holsters.) All screening staff should be trained and outfitted with non-lethal defense equipment. All screening staff should have body cameras and radio communication equipment.
28. If two or more public screening stations are in operation, assign a fourth CSO as a supervisor to oversee operations.
29. Install a magnetometer, x-ray imaging system, duress alarm, and security camera at the judge/staff entrance. Consider allowing jurors to use this entrance.

30. Assign at least two security officers (at least one of whom should be a CSO) to the judges/staff entrance if staff or jurors use this entrance and at peak hours during the day. Otherwise, assign at least one CSO.

31. Establish a universal screening policy. Universal screening means everyone entering the building is screened. (However, if there is not a separate entrance with a screening station for judges, then judges ought not to wait in a screening line at a public entrance.)

**Note: Staffing level in Best Practice is three full-time security officers for each public screening station, at least two of whom should be CSOs. There should also be one additional CSO to supervise multiple stations, and two security officers (at least one of whom should be a CSO) assigned to judge/staff/juror entrance.*

Best Practice Elements of Screening Stations

- Two magnetometers for each x-ray machine
- Three full-time security officers for each public screening station, at least two of whom should be CSOs
- Adequately sized for volume of traffic
- Appropriate queuing lanes
- Clear and separate entry and exit lanes
- Ballistic-resistant vests and shields
- Security camera
- Duress alarm
- Tables/chairs located away from screening station for people to get themselves back together after screening

TOPIC B-6: PUBLIC SERVICE AREAS, COUNTERS, AND OFFICES

PHASE ONE

1. Install one or more duress alarms at each public counter. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in offices (e.g., drapes, blinds) drawn to restrict observation from outside.
3. Install Plexiglas™-type enclosures at cash counters.
4. Keep cash and checks in a secure, locked area overnight.
5. Ensure all counters are designed with adequate height and depth dimensions to discourage and limit attempts to jump or climb over.
6. If there are chairs provided in a public seating area near the counter, make sure that the chairs are fastened to the floor or tied together.

PHASE TWO

Continue all steps in Phase One, plus add the following:

7. Install polycarbonate (e.g. Plexiglas™) barriers over all public counters. If there is no screening station at the court building, or if screening is materially deficient, ballistic-rated barriers should be above the counter as well as below the counter.
8. Install duress alarms strategically in the back areas of offices.
9. Install duress alarms in all mediation and conference rooms. Position furniture in mediation and conference rooms with security in mind. For example, staff's access to the exit door should not be blocked by a visitor's chair.
10. Keep cash and checks and daily change locked in a safe overnight.
11. Establish safe room(s) in the courthouse where judges and staff can seek safety in the event of a negative event. Retrofit the locking mechanism on the door so that it can be locked and unlocked from the inside. Reinforce the door jamb to protect against the door being kicked in. Install a duress alarm in the safe room.
12. Provide mobile duress alarms to staff who must share restroom facilities with the public.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

13. Install security cameras at the back of all public counters to capture the faces of members of the public conducting business at the counter.
14. Install appropriate alarms and sensors (i.e. security, smoke, fire, extreme moisture, and motion) on safes.
15. Provide safe and secure waiting areas for victims and witnesses, those seeking protective orders, and other members of the public who might be at risk of assault.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

16. Install a security camera overlooking all safes.
17. Require scheduled patrols of all interior areas 24/7.
18. Install doors with glass panes and sidelight windows in all mediation and conference rooms.

TOPIC B-7: JUDGES PARKING

PHASE ONE

1. Remove all signs in judges' parking areas that identify parking spaces either by name or title of judge. Any signs should simply say reserved along with a number as appropriate.
2. Judges should notify law enforcement officials or a designated CSO of their arrival in the morning and be offered an escort if they park in an unsecured parking area.
3. When departing for the day, if requested, judges should be provided an escort to unsecured parking areas by designated CSOs.

PHASE TWO

Continue the steps in Phase One, plus add the following:

4. Fence-in the judges' parking lot using opaque materials such as brick or stone. If this is not feasible and instead a chain-link fence is used, install privacy slats in the chain-link.
5. Make sure that in-custody defendants are never afforded a view of judges getting in or out of their vehicles.
6. Install adequate lighting at the parking lot.
7. During high-threat proceedings and heightened security concerns, judges should be escorted to their vehicles and other modes of transportation.
8. Ensure the judges' parking area is equipped with appropriate security and safety lighting. Reference B-8 for additional lighting information.
9. Calibrate the timing of doors or gates to secure parking areas so that the doors or gates do not remain open for too long of a period of time.

PHASE THREE

Continue the steps in Phases One and Two, plus add the following:

10. Install call boxes and security cameras in the parking lot.
11. Provide judges and court staff a regular CSO patrol presence in the parking areas in the morning, during the lunch hour, and at close of business.
12. Install passive and active security barriers to parking areas, accessible by way of an access card or other appropriate device.

BEST PRACTICE

Continue the steps in Phases One, Two, and Three, plus add the following:

13. Provide a secure parking area, preferably covered, for judges where they can proceed directly from their car, through screening, to their chambers without traversing any public areas or main court building entrance areas.

TOPIC B-8: PERIMETER ISSUES

PHASE ONE

1. Install appropriate signage to alert the public to what items cannot be brought into the court building (i.e., guns, knives, scissors) and that all persons are subject to search by security.
2. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness. It should also be sufficient for perimeter security cameras to capture images.
3. Keep doors locked after hours and allow access only via appropriately authorized key or access cards.
4. Employ a sound crime prevention program through environmental design by properly maintaining landscaping, trees, and shrubs to limit areas of concealment and prevent property damage and undetected access.
5. Conduct daily security checks around the perimeter, particularly at times when the building is closed.
6. Install signage to indicate any areas that are restricted to public access.
7. Relocate all trash receptacles, newspaper kiosks, and any other items that could be used to conceal weapons or hazardous materials to a safe distance away from the court building.
8. Make sure that there are clear, open, and non-congested lines of sight for all areas around the perimeter of the court building.
9. Make sure that there is adequate and unobstructed space for evacuation of the court building and for unfettered access by first responders.

PHASE TWO

Continue steps in Phase One, plus add the following:

10. Install intrusion detection systems to cover all exterior doors and accessible windows.
11. Assign CSO exterior patrols both regularly and randomly throughout the day.
12. Use window coverings and ballistic-resistant material on windows to minimize the risk of someone assaulting building occupants from the outside.

PHASE THREE

Continue steps in Phases One and Two, plus add the following:

13. Install security cameras around the perimeter (at each corner of the court building). Make sure that security cameras have a clear line of sight around the entire perimeter of the court building.
14. Install bollards as required outside selected main entrance doors, shipping and delivery docks, over-sized ground floor windows, and other vulnerable or critical areas.
15. Prohibit motor vehicles from parking or accessing areas adjacent to or within “blast-proximity” of the court building.
16. Enclose and secure all exposed gas, electric, and other utilities from public access or tampering. Secure air ducts or other openings from physical intrusion and from the introduction of any toxic substance.
17. Require scheduled patrols of all exterior areas 24/7.

BEST PRACTICE

Continue steps in Phases One, Two, and Three, plus add the following:

18. Install reflective glass so that the public cannot see into the front entrance screening area, but that the screening station staff can see outside.
19. Replace keys with an electronic card access system (except for back-up emergency) on exterior door entrances to the court building.
20. Install emergency call boxes in both staff and public parking areas around the court building.

CATEGORY C: ESSENTIAL

TOPIC C-1: AFTER-HOURS ACCESS TO COURT BUILDING

PHASE ONE

1. Permit access into all areas of the court building only via key or electronic card access. Keys and cards should be issued and controlled pursuant to a comprehensive accountability system that has been approved under the purview of the court building security committee.
2. Conduct background checks prior to issuing a key or access card to any person. Background checks should be conducted prior to employment or execution of a contract. All after-hours access should be restricted as much as possible. Good security should not be set aside for convenience.
3. Conduct annual background checks for cleaning crews and any vendors granted after-hours access to the building. Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court. To the extent possible, courtrooms and chambers should be cleaned by crews/vendors during the business day with no authorized access after-hours. Cleaning crews should never be allowed to work in judges chambers' alone.
4. Document and monitor those activities where the public is required to be in the building after-hours. Set policies and procedures to ensure no unauthorized persons are in the building after-hours.
5. When anyone's employment is terminating, access cards should be inactivated and keys turned in on the last day that the card or key holder is present in the court building. Make sure that this has happened prior to the issuance of a final paycheck.

PHASE TWO

Continue all steps in Phase One, plus add the following:

6. Eliminate the use of keys and implement the use of an access card system. Where keys are required in specific instances, issue double-cut, non-duplicate keys for use in emergencies or building maintenance purposes.

BEST PRACTICE

Continue all steps in Phases One and Two, plus add the following:

7. Create a single access point into the court building that is secured by a CSO, or contract security officer, who checks identification and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
8. Conduct full security screening operations requiring all persons to go through entryway screening.

TOPIC C-2: EMERGENCY EQUIPMENT

PHASE ONE

1. Install an emergency, battery-generated lighting system in courtrooms, offices, and public areas.
2. Install a fire extinguisher on each floor, with egress floor plans posted.
3. Install fire alarms on each floor.
4. Install an elevator(s) that meets all applicable and updated fire codes.

PHASE TWO

Continue all steps in Phase One, plus add the following:

5. Install an emergency generator system that is properly fenced-in and protected.
6. Test generator system monthly; keep a log of tests.
7. Determine the time-delay for emergency generators to “power-on” and install uninterruptible power supplies (UPS) for critical systems.
8. Install automated external defibrillators (AEDs) located accessibly on each floor of the court building.

BEST PRACTICE

Continue all steps in Phases One and Two, plus add the following:

9. Ensure the fire alarm system is equipped with both a strobe and annunciator per code.

TOPIC C-3: INTRUSION DETECTION SYSTEMS

PHASE ONE

1. All exterior doors should have basic intrusion alarm devices, covering:
 - Building ingress/egress during business and after-hours.

- Emergency exit doors during business and after-hours.

PHASE TWO

Continue the step in Phase One, plus add the following:

2. Install intrusion devices on all accessible windows, either glass-break or motion sensors, on the basement, first floor, and possibly the second floor. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

3. Establish a fully integrated intrusion system with the following functionalities:
 - When a court building is closed, every external door should be equipped with a device that will trigger an alarm at the command center of the appropriate responding agency and identify the intruded area.
 - During business hours, every door that is kept locked should be equipped with a device that will trigger an alarm that will identify the area intruded at the command center within the building. Every locked door with an emergency exit bar should trigger an alarm whenever anyone uses it, with a ten-second delay consistent with local codes.
 - When the building is closed, the alarm should go to the control center of the appropriate responding law enforcement agency; when the building is open, the alarm should go to the building's command center.
 - Intrusion detection alarm systems should sound locally at the site of the alarm and also at the command center (or at a 911 dispatch center if the court building command center is not staffed when the court building is closed).

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

4. Integrate security cameras into the system described above so that cameras will be activated in the area(s) of intrusion.

TOPIC C-4: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES)

PHASE ONE

1. Establish, as feasible within the courthouse, the concept of circulation zones (separate, restricted, and secured areas and routes) for the following:
 - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, staff-side of public counters, private elevators, secure stairways).
 - In-custody defendant transport (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms).
 - Public (e.g., restrict the public to public zones).
2. All doors that are required to be locked, in accordance with the court building circulation zone concept should be kept secured at all times. Such doors should never be left propped open and unsecured.
3. Have a key or access card system to control access based on a system approved by the administrative authority of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience. Keys should be double-cut and not subject to duplication. This system should:
 - Be under the control of a central authority.
 - Require background checks for all card or key holders.
 - Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination).
 - Require an up-to-date inventory on all access cards and keys.
4. Require, when employment is terminated, that cards be inactivated and keys turned in on the last day that the card or key holder is present in the court building, and to ensure that this has happened prior to the issuance of a final paycheck.

PHASE TWO

Continue all steps in Phase One, plus add the following:

5. Eliminate keys and require access cards. Maintenance staff and emergency responders should retain keys.
6. Include sufficient information on the face of the access card to allow a security officer to challenge the person in possession of the card in order to make sure that the person is in fact the properly authorized holder of the card. In this regard, it is helpful for face of the access card to contain a photograph of the authorized holder.

7. Establish door scopes (peepholes) to prevent non-authorized access through secured courtroom doors.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

8. Establish a video intercom and remote controlled magnetic door strike system to allow access into secure areas.
9. Continue to improve definition and enforcement of circulation zones.
10. Install a security camera system in all secure areas of the court building to monitor suspicious activities and inappropriate or threatening behaviors.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

11. Establish and maintain complete separation among zones (e.g., in-custody defendants are not escorted through secure or public hallways; judges do not pass through public areas when going to and from their cars, through screening, and to and from chamber areas). As warranted, security zones should run vertically (floor to floor) as well as horizontally (on the same floor).

TOPIC C-5: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

PHASE ONE

1. Provide emergency lighting in the court building including backup generator powered lighting and lighted emergency egress signage.
2. Establish egress/ingress standards regarding stairwells, hallways, and elevators. For most court facilities, there should no re-entry for persons exiting into stairwells. Entry from the stairwell-side should be by controlled access only. For court buildings considered “high-rise” facilities, certain floors, as determined via security assessment and life safety analysis, may allow for re-entry.
3. Establish emergency procedure and evacuation diagrams. Post floor diagrams in hallways of the court building.

PHASE TWO

Continue all steps in Phase One, plus add the following:

4. Designate secure and public elevators.
 - Provide secure elevator(s) for judges.
 - Provide a secure elevator for in-custody defendant transport.
5. Conduct regular CSO interior patrols by CSOs assigned to work in the court building, focusing on crowded hallways.

BEST PRACTICE

Continue all steps in Phases One and Two, plus add the following:

6. Install security cameras in court building lobbies, hallways, stairwells, elevators, and at elevator landings. Provide secure elevator(s) with electronic card access.
7. Assign a CSO to regularly patrol these areas in accordance with an assigned schedule.
8. Install a public address system in the building to facilitate announcements and emergency codes.

TOPIC C-6: JUROR SECURITY AND CIRCULATION

PHASE ONE

1. Provide jurors with court security information before they report for duty by placing information on the jury summons they receive. For example:
 - Where to enter the court building.
 - What items (e.g., knives, nail files, scissors) may not be brought into the court building.
 - Not to discuss cases with anyone before and during jury service.
 - Not to wear juror identification badges outside the court building.
 - Who to contact regarding security and safety concerns or jury tampering.
2. Screen jurors as they enter the court building or before they report to the jury assembly area.
3. Give a basic security and building evacuation orientation and identification badge to jurors at the assembly area before going to the courtroom. Cover such matters as what to do in case of an emergency and how to respond to a coded emergency announcement. Instruct jurors to not wear or display the identification badge off-site; and whom to notify if it is missing or lost.
4. Assign a CSO or bailiff to remain with the jury during the entire trial and outside the deliberation room.

BEST PRACTICE

Continue all steps in Phase One, plus add the following:

5. Assign a CSO to provide security inside and outside the jury assembly room when jurors are present.
6. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervisor the loading of jurors and another CSO should meet the jurors on the floor on which they disembark.
7. Install a duress alarm in each jury deliberation room and in the jury assembly room.
8. Provide restrooms for juror use only, with no public access.
9. Provide secure ingress and egress for jurors to the court building and to their vehicles to avoid the threat of intimidation or attempt to influence.

TOPIC C-7: CASH HANDLING

PHASE ONE

1. Develop and train court staff on procedures for handling cash. The procedures should:
 - Determine who should collect the money.
 - Determine how to safeguard money during the daytime work hours and overnight.
 - Train staff on how to verify checks and reconcile fees.
 - Determine and implement industry standards for deposits.
 - If employees are responsible for depositing funds, vary scheduled departure times and routes and employees assigned; and notify designated persons when departing for and completing the deposit.
2. Install protective barriers and duress alarms at cash counters.
3. Use a securely-installed office safe for money storage.

PHASE TWO

Continue all steps in Phase One, plus add the following:

4. Install security cameras at counters and in offices where cash is handled.

PHASE THREE

Continue all steps in Phases One and Two, plus add the following:

5. Use an armored car service or the bank's personnel to pick up funds daily.

BEST PRACTICE

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require two people – one court staff and an armed CSO – when carrying cash in and/or out of the court building.

TOPIC C-8: SCREENING MAIL AND PACKAGES

PHASE ONE

1. Provide routine visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items.
2. Require staff to attend training on postal security, recognition points, and package identification techniques as provided by the United States Postal Service (USPS).
3. Develop and practice a response protocol with law enforcement when a package is identified as suspicious or dangerous.
4. Develop specific policies and procedures to confirm mail/package senders and recipients, and whether the mail/package has been tampered with.

PHASE TWO

Continue all steps in Phase One, plus add the following:

5. Require all mail and packages to be processed through an x-ray imaging system.
6. Require everyone delivering mail or packages to pass through the magnetometer.

BEST PRACTICE

Continue all steps in Phases One and Two, plus add the following:

7. Establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:
 - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious)

upon being received at the mailroom. This includes all USPS mail delivered and picked up by court staff from the local post office.

- Deliveries of flowers, candy, food, gifts, etc., to any person located in a court building should be cleared through the mailroom first, be verified and vouched for by the recipient, screened as appropriate, and then delivered.
- Mailroom staff should sort incoming mail and packages off site by building, division, and/or department and prepare them for acceptance by designated representatives of each court office or division.
- Designated representatives of each court office or division should go to the mailroom, pick up mail for distribution to their offices, and identify questionable items. All authorized court and other staff mail handlers should attend training on handling suspicious mail. Local USPS or postal inspectors may conduct advanced training for state and local government agencies.

STAFFING, DURESS ALARM, AND SECURITY CAMERA RECOMMENDATIONS INCLUDED IN THE BEST PRACTICES

NOTE: Staffing, duress alarm, and security camera recommendations summarized here have been previously described in the steps, phases, and categories listed previously.

COURT SECURITY OFFICER (CSO) STAFFING LEVELS

A CSO, as referenced in this document, is defined as an individual trained and qualified in court building security, and has been specifically trained and qualified to use a firearm and intermediate weapons, e.g., Taser, chemical spray, or restraints (i.e. handcuffs, leg restraints). An armed CSO should be outfitted with a triple-retention holster. All CSOs should be outfitted with a radio that can communicate with the command center and a body camera. The CSO assigned to the command center is not necessarily required to carry a firearm.

1. One CSO should be permanently assigned to the main entrance of the court building during business hours.
2. One CSO or transport deputy should be assigned to the courtroom while there is an in-custody defendant in the courtroom.
3. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a rover from one courtroom to the next. There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.

Note: It is estimated that each CSO post requires an appropriate relief factor. Typical relief factors range from 1.2 to 1.3 full-time employees to cover for sick and annual vacation, training, etc.

4. As additional CSOs become available, assign in the following priority per recommended phases leading up to best practice level in each relevant topic:
 - To meet recommended staffing guidelines at screening station (Topic B-5).
 - To meet recommended staffing guidelines for the courtroom (Topic B-3).
 - To meet recommended ratios for transporting in-custody defendants (Topic B-2).
 - To assign patrols for the interior and exterior of the building (Topics B-8 and C-5).
5. Achieve full recommended staffing guidelines for the following topics:
 - Screening stations (Topic B-5).
 - Courtrooms (Topic B-3).
 - Transporting in-custody defendants (Topic B-2).
 - Regular patrols of building interior and exterior (Topics B-8 and C-5).

DURESS ALARMS

1. Install duress alarms in the courtroom and at the bench, clerk's station, and CSO station. Training should be provided on the functionality of duress alarms and on the protocols for use (Topic B-3).
2. Alarms should be tested at least monthly. Alarm batteries should be tested semi-annually.
3. Install alarms in each chamber and reception area (Topic B-4).
4. Install alarms at screening stations (Topic B-5).
5. Install alarms at public counters, cash areas, and other offices where the public has access, including those without counters (Topic B-6).
6. Provide mobile duress alarms to staff who must share restroom facilities with the public (Topic B-6).
7. Install alarms in the interview and mediation rooms that are used by members of the public.
8. Install alarms and 911 contact ability at the childcare center, if the court building includes such a center.
9. Install an alarm in the jury assembly room and in each jury deliberation room (Topic C-6).
10. Install duress alarms in the holding cell area.
11. Install a duress alarm in the loading dock area (Topic B-8).
12. Install a duress alarm in the mailroom.
13. Integrate duress alarm and camera systems so the closest security camera is automatically activated for monitoring and recording when alarms sound.

SECURITY CAMERAS

Security cameras should have the following functional capacity:

- Capacity to focus on targeted areas. Two types of cameras that have traditionally been used at court buildings are (a) pan/tilt/zoom cameras, and (b) fixed cameras. More recently, high-definition digital cameras with wide angle lenses and digital pan/tilt/zoom capability have become popular and in some places have supplanted the use of more traditional pan/tilt/zoom cameras. Wide angle cameras, when equipped with sufficient image resolution quality, provide the capability for the user to focus digitally on targeted areas without losing the overall wide angle coverage provided by the camera, thus avoiding the limitations inherent to traditional pan/tilt/zoom cameras (i.e., pan/tilt/zoom cameras might be panning and zooming at location X while another event may be happening at location Y).

- Color. This is standard in current systems. Black-and-white images cannot tell the full story. Important features are indistinguishable. Only with a color monitor can faces and other specific objects be clearly identified.
- Network streaming capacity. Security systems can utilize various kinds of technology to transmit video images and to provide system access and control. Many systems now utilize an internet protocol (IP) to transmit data and control signals over a network using a broadband link providing access to CSOs, first responders, and court personnel. Courts are encouraged to explore and adopt the ever advancing new technologies that best suit their needs and budgets.
- Recording capacity. The camera system should have digital video recording capacity enabling a CSO to view incidences at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation capacity. The operation and recording function of a camera can be set to activate by either motion or sound, or by setting off duress or intrusion alarms.

Security cameras should be installed in the following locations:

1. Security camera notification signage should be conspicuously placed to inform the public that security cameras are operating and recording activity in the area.
2. Install a digital and color security camera system at the entry screening station and in the courtroom(s) facing the gallery.
3. Install security cameras (with tamper-resistant housings) in detention areas to monitor activities in holding cells and in-custody defendant circulation areas (Topic B-2).
4. Install security cameras with protective environmental housings on the court building perimeter. Use the camera system to detect suspicious activities and incidents, and to monitor parking and adjacent areas (Topic B-8).
5. Install security cameras to monitor activity at public counters and in offices where the public may visit (Topic B-6).
6. Install security cameras at the loading dock (Topic B-8).
7. Install security cameras in hallways (Topic C-5).
8. Install security cameras in each courtroom (Topic B-3).
9. Install security cameras in elevators and stairwells (Topic C-5).
10. Install additional security cameras at security screening stations (Topic B-5).
11. Install security cameras in hallways that access chambers (Topic B-4).
12. Install security cameras in the mailroom.
13. Install security cameras in the childcare area, if such an area exists.

14. Install security cameras to cover all pathways through which an in-custody defendant may be escorted (Topic B-2).

CONCLUSION

Operating a courthouse today is by its very nature a risky business. Day in and day out, courthouses are visited by a large volume of disgruntled and even law-breaking citizens. Moreover, courthouses can be seen as an important symbolic target for those in our midst who wish to wreak mischief or terror.

Courthouse security is not a one-time achievement. It is a serious and continuous goal requiring constant vigilance. Security is a total team effort. Every court employee is an integral part of the “security team.” From court clerks, to county employees, to law enforcement officers, every person has a role. “See something, say something” must be the constant mantra. Judges need to be actively involved and supportive of the security effort. When judges are committed to security, a trickle-down effect on court employees will follow. When judges are not supportive of security, staff never will play their full necessary role in security efforts. The leadership role of judges cannot be overstated. Further, security must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and generally can never be eliminated. However by exercising due diligence and devoting the appropriate attention, incidents can be both minimized and mitigated. Adhering to the stated principles and recommendations contained in this *Steps to Best Practices for Court Building Security* document will greatly assist the courts in this regard.



Courts Continuity of Operations (COOP) Planning Guide and Template

Nathan Hall, Project Director
Justin Mammen, Project Consultant
Steven Berson, Project Consultant
Greg Cowan, Project Consultant
Felix Bajandas, Project Consultant

Daniel J. Hall, Vice President
Court Consulting Services
707 Seventeenth Street, Suite 2900
Denver, Colorado 80202-3429





© 2021

National Center for State Courts

This document was prepared under State Justice Institute (SJI) Grant #SJI-18-T-045. The points of view and opinions expressed in this document are those of the author, and they do not necessarily represent the policy and positions of the State Justice Institute. The National Center for State Courts grants the State Justice Institute a royalty-free, non-exclusive license to produce, reproduce, publish, distribute or otherwise use, and to authorize others to use, all or any part of these documents for any governmental or public purpose.

The publication of this guide and template has been made possible by the cooperation and hard work of many people. A special thanks is offered to the COOP focus group participants whose lessons learned and experiences from major disasters greatly informed the content of this guide and template. Also, FEMA is acknowledged both for the resource materials that have helped to inform many portions of this guide and template as well as for the participation of its representatives throughout the course of the NCSC project. Additional thanks is offered to the members of the CCJ/COSCA Joint Committee on Court Security and Emergency Preparedness who have supported the NCSC's work in this area and have provided valuable advice throughout all of the initiatives included in this grant.

Nathan Hall, NCSC Principal Court Consultant, directed this important project. The NCSC consultant team on this project included Felix Bajandas, Steven Berson, Greg Cowan, and Justin Mammen. Special recognition is offered to Justin Mammen, who was relied on extensively as a primary subject matter expert during the development of the guide and template.

CONTENTS

INTRODUCTION	1
COOP PLANNING BASICS FOR STATE COURTS.....	3
SECTION I: INITIATING THE PLANNING PROCESS.....	5
SECTION II: WRITING THE PLAN	10
PART A: READINESS AND PREPAREDNESS.....	11
PART B: ACTIVATING COOP IN A DISASTER OR EMERGENCY	37
PART C: ONGOING COOP OPERATIONS DURING A DISASTER OR EMERGENCY.....	39
PART D: RECONSTITUTION AND COST RECOVERY.....	41
SECTION III: FURTHER COOP CONSIDERATIONS	45
TRAINING AND EXERCISE PROGRAMS	45
DEVELOPING ANNEXES	47
SAMPLE PANDEMIC ANNEX FOR A NOVEL VIRUS	49
ADDITIONAL RESOURCES	53
APPENDIX: COOP TEMPLATE	54
COOP TEMPLATE - PART A: READINESS AND PREPAREDNESS.....	55
COOP TEMPLATE - PART B: ACTIVATING COOP IN A DISASTER	67
COOP TEMPLATE - PART C: ONGOING COOP OPERATIONS DURING EMERGENCIES	68
COOP TEMPLATE - PART D: RECONSTITUTION AND COST RECOVERY	69
COOP TRAINING AND EXERCISE PROGRAM IDENTIFICATION WORKSHEET.....	71
COOP HAZARD ANALYSIS WORKSHEET.....	72
COOP HAZARD ANNEX TEMPLATE.....	73

INTRODUCTION

State courts in this country provide important “mission-essential functions” that are critical to maintaining the rule of law and providing justice and equal access for the fair and timely resolution of cases and controversies. It is imperative that these essential functions not be disrupted or compromised during or after a natural disaster or other emergency. Given the critical nature of these functions, the development of a Continuity of Operations (COOP) plan is crucial for courts to continue their mission-essential operations in the face of a natural disaster or emergency.

The development of a COOP plan can be a daunting, time-consuming assignment, one that competes with the myriad other responsibilities facing court officials and staff. This Guide is designed to be user-friendly and to make developing a COOP plan less daunting. It offers clear step-by-step instructions. Following all the steps and providing the information requested at each step will ultimately yield a complete and comprehensive COOP plan at the end of the process.

This Guide is designed to assist both seasoned court emergency managers and as well as court staff with little or no emergency management experience. Regardless of experience, this Guide will help whoever has been assigned as the COOP point person tackle this endeavor one step at a time.

ABOUT THIS INITIATIVE

This Guide was produced by the National Center for State Courts (NCSC) under a grant from the State Justice Institute (SJI). The SJI grant was awarded to fund the production of new court-centric materials to help courts function during an emergency or disaster. There were four “initiatives” contemplated under the grant.

The first initiative under the grant was the convening of an Emergency Management Lessons Learned Focus Group in Denver, Colorado to study: (1) what courts experiencing a recent natural disaster had previously put in place in terms of COOP planning and emergency management resources; and (2) how their respective positioning and planning affected their ability to respond to their respective disasters. The goal of the focus group was to provide an opportunity to share experiences and leverage the expertise of key court officials to improve state courts’ performance in the areas of emergency management and continuity of operations planning. A final report with recommendations from this focus group can be found on the NCSC website.

Under the second grant initiative, the NCSC provided direct technical assistance to each of the focus group participants, evaluating and providing recommendations to the court’s emergency management programs in the jurisdictions who participated in the focus group.

The third grant initiative includes this COOP Guide, which replaces the NCSC’s “Steps for COOP Planning” developed in 2007. This Guide reflects current trends in emergency management, technology, as well as all the lessons learned from the first initiative focus group. The fourth initiative under the grant will focus on the development of COOP specific tools/technology to assist courts in their continuity program.

HOW TO USE THIS GUIDE

This Guide is organized into the following three sections and one appendix:

Section I – Initiating the Planning Process. The process of planning for COOP is just as important as the plan itself. Section I includes a series of steps that a court should undertake to initiate the COOP planning process.

Section II – Writing the Plan. This section includes steps that will guide the court through the key elements needed for its COOP plan.

A discussion of important COOP considerations is included with each step presented. Each step also includes one or more tables for use in capturing and organizing important COOP guidance and information. These tables have been pre-populated with sample language based on a hypothetical court. Users of this Guide may choose to copy the sample language included in the tables for use developing their own COOP plan using the COOP template included in the Appendix of this guide. Hyperlinks are included to help navigate from the pre-populated tables in Section II to the corresponding blank table located in the COOP Template.

Entering information in the COOP Template, in effect, constitutes writing the court's COOP plan. When completing the tables, the examples provided may prove relevant; however, planners should assess if the pre-populated information is appropriate and relevant for their specific court system. This pre-populated information has been added to make the process of completing a COOP plan as painless and straightforward as possible; however, it must be pointed out that the process of completing a COOP plan is typically highly involving. Writing the plan as detailed in Section II will be the most time-consuming aspect of COOP planning covered in this Guide, but the effort put into it will prove to be extremely helpful in the future when the court faces a disaster or emergency.

Section III – Further COOP Considerations. This section covers important COOP items that should be considered following the completion of a base COOP plan as outlined in Section II. These include the following:

- **Training and exercising the plan.** This portion of the guide reviews the establishment of training and exercise programs that are needed to integrate the COOP plan into the culture of the court system. A robust training and exercise program can help ensure the plan becomes a living document rather than a binder collecting dust on a shelf.
- **Developing annexes.** This last portion of the guide reviews the identification and development of annexes to the court's base COOP plan. Annexes are typically developed to address unique hazards that are not specifically addressed in detail within the base COOP plan. Section III includes both a Hazard Analysis tool for the identification of needed annexes and a sample Pandemic Annex which may be used by the users of this Guide in the same manner discussed above.

Section III, like Section II, includes multiple pre-populated tables for use in inputting information. Hyperlinks are included to help navigate from the guidance in Section III to the COOP Template.

COOP Template (Appendix). A blank COOP Template is included as an Appendix to the Guide. As mentioned above, COOP planners may choose to use the sample language included in the Guide to complete their COOP plan as appropriate for his or her own court.

COOP PLANNING BASICS FOR STATE COURTS

COOP is defined by the Federal Emergency Management Agency (FEMA) as an effort within an organization to ensure its essential functions continue to be performed during a wide range of emergencies. Typically, a COOP plan will be utilized when a court is faced with a major crisis that impacts its ability to perform all its various functions. Thus, when courts face a continuity scenario, they must focus solely on what is essential and not necessarily on all the various proceedings and services normally provided.

As seen in recent history, courthouses are not immune to disasters. Whether it be terrorism (e.g., 9/11), fires (e.g., California wildfires of 2017 and 2020), hurricanes (e.g., the 2017 and 2018 hurricane seasons) or the global COVID-19 pandemic in 2020, courts can be severely impacted by both natural and human-caused disasters. Despite this, courts have a constitutional duty to ensure their continuity of operations during a crisis.

CONTINUITY OF GOVERNMENT AND COOP FUNDAMENTALS

Another term often used in a continuity event is the “Continuity of Government” (COG). COG is a coordinated effort within the three branches of government to ensure that essential functions continue to be performed before, during, and after an emergency or threat. Thus COG, within the judicial branch, relies on local and state courts having a viable continuity capability based upon good planning. To maintain our enduring constitutional government, courts must be ready for these continuity situations with a functional and updated COOP plan.



Image from FEMA CGC (2018)

A court’s COOP plan should not be the only emergency planning document it has. Many courts have other emergency plans such as its Emergency Operations Plan, Evacuation Plan, and/or IT Disaster Recovery Plan. A court’s COOP plan must ensure it both complements and supports its other emergency plans and planning efforts.

COOP forms the foundational structure of how courts can continue their essential functions in an emergency. It sets the framework that can be applied to every disaster. To provide more specificity and protocols to specific threats/hazards, courts should consider developing annexes. Each disaster scenario can bring nuances to a court’s response. Thus, development of annexes after completion of this overarching COOP plan can be helpful to address these specific nuances that come up in disasters (e.g., for earthquakes, define how building seismic evaluations would occur post-earthquake; for hurricanes, name what specific steps need to be taken once a hurricane watch is reported by the National Weather Service). Developing annexes is discussed at the end of Section II of this document.

When disasters occur, our communities turn to the three branches of government to ensure their safety and security. Thus, the development of a COOP plan is vital for courts. Developing a plan will not be completed overnight. The planning process will take time, but it is every court’s duty to ensure this planning occurs so that when the time comes and the court is faced with a disaster, it stands ready to respond.

COOP PLANNING IN UNIFIED AND NON-UNIFIED COURT JURISDICTIONS

COOP planning will vary across jurisdictions depending on the number of courts operating independently in a jurisdiction and the number and types of court facilities involved. For purposes of this Guide, “court” refers to all the judges, court staff, and facilities under the authority of the Presiding or Chief Judge. In some jurisdictions, all courts are unified under a single leadership structure. In others, the general and limited jurisdiction courts may

not be unified. In the latter scenario, the Presiding or Chief Judge of each court should make sure that COOP planning takes place for his or her respective jurisdiction. In locales where multiple independent court COOP plans are developed, it is strongly recommended that representatives from the different courts review the various plans with each other. This is done to ensure compatibility among the plans, coordination of available resources, and to promote the sharing of knowledge. The COOP Template presented in this Guide provides a framework for a single plan that covers an entire court system. It will be up to each court system to determine if this structure works or if individual continuity plans are needed for each courthouse.

COOP PLANNING AND COURT FACILITY CONSIDERATIONS

Court facilities also vary by jurisdiction, and the composition of how facilities are arranged and managed will impact COOP planning. In some jurisdictions, all court-related functions occur in a single building under the control of the judicial branch. In others, the functions occur in a county-owned building that might be shared with executive branch agencies. In yet another scenario, functions are spread across the jurisdiction in several facilities that might or might not be under the authority of the judicial branch.

The COOP plan needs to consider the court's unique facility composition to provide a coordinated framework for directing all judges and court staff's efforts. A COOP plan is needed even in situations where the court does not own or maintain its own facilities and shares space with other non-court entities. This will ensure, to the extent possible, that essential court functions are compatible with the COOP plans of those other entities.

SECTION I: INITIATING THE PLANNING PROCESS

As stated previously, the planning process is just as important as the written COOP plan itself. A continuity plan is not written overnight, nor can it be developed entirely by a single person. Thus, COOP planning is a cross-functional and collaborative team effort. Relationships are key and form the foundation of the planning process. Therefore, getting the right stakeholders to the planning table to develop the plan is critical.

STEP 1-1: GAIN EXECUTIVE SUPPORT

Writing or updating a COOP plan is a major undertaking and should be treated with the same importance as rolling out a new case management system. It will require time and effort from all court departments/divisions as well as external stakeholders. Having the support of the Presiding or Chief Judge and the Court Administrator is critical to ensure the right people and amount of time are devoted to this project. The Presiding or Chief Judge and the Court Administrator will need to appoint a “COOP Planner” referenced in Step 1-2 and assemble a “COOP Planning Team” referenced in Step 1-3.

It may be beneficial to appoint an executive liaison to help along the way. This can be helpful when the planning process encounters roadblocks (e.g., a department that is not participating in the planning process or two departments that want to take a vastly different approach) to ensure the planning process stays on track.

STEP 1-2: ASSIGN A “COOP PLANNER” AND PROVIDE NECESSARY TOOLS FOR THE JOB

A COOP Planner should be identified to lead the court’s efforts in developing its COOP Plan. The assigned person should have good project management experience and should be in a position of authority or have the delegated authority to call meetings, set deadlines, assign tasks (often to those who are in a more senior position). Though this process will require a team effort, as noted below, the COOP Planner will be the person in charge of running the project and putting the plan together.

As the COOP Planner goes through the steps in this Guide, a large amount of information will need to be gathered. There will be many documents to sift through, and revision control on electronic documents is important. Having a common virtual work area (e.g., SharePoint, Dropbox, Google Drive, etc.) to store and access these could prove beneficial.

Ideally, the COOP Planner should be someone who knows the various departments of the court. Preferably the Planner will be someone with an emergency management background. Though preferable, this is not necessarily a requirement. There are resources, training, and tools to assist court staff in gaining the knowledge to help put together a plan. The [FEMA National Continuity Programs](#) offer a variety of resources to support anyone putting together a COOP plan. Online classes can be found at the [FEMA Emergency Management Institute – Independent Study website](#). FEMA also offers in-person COOP training courses. A list of all COOP related training can be found on the [FEMA training website](#). Courses pertaining to continuity of operations, reconstitution, devolution, and pandemic planning can prove beneficial.

FEMA training is typically provided at no cost to the court. Connecting with FEMA Regional Continuity Coordinators and/or local emergency management office can also help a planner get trained to develop a COOP.

STEP 1-3: ASSEMBLE THE COOP PLANNING TEAM

The development of a court COOP plan is a serious and involved endeavor that will likely require the attention and expertise of other personnel beyond just the COOP Planner. A COOP Planning Team should be assembled to advise and assist the COOP Planner in developing the plan. The COOP Planning Team should include representation from all major court departments. Examples of possible departments represented:

- Facilities
- IT
- Courtroom Operations
- Case Processing
- Jury Operations
- General Counsel
- Finance
- Procurement
- Accounting
- Human Resources
- Security (e.g., County Sheriffs, Court Marshals, Court Security Contractors, etc.)

Ideally, a planner will need at least one representative from all major departments who will serve as the COOP lead for their respective area/department. Ultimately, for the scope of the COOP plan development, the COOP Planner will oversee the COOP Planning Team.

Inviting a judge or multiple judges to participate on the planning team is helpful to help convey the needs of the bench to the team, and to promote the importance of the COOP program with other judges. Courts should also consider assigning an executive liaison to the COOP Planning Team such as a respected Judge, the Court Administrator, or other senior official. The liaison's role is to be a champion for the team and help advocate for the resources needed to complete the plan. The liaison can also be helpful when the planning process encounters roadblocks (e.g., a department that is not participating in the planning process or two departments that want to take a vastly different approach) to ensure the planning process stays on track. If time does not permit the liaison to attend all planning meetings, the planner should ensure the liaison is kept aware of the planning team's progress, successes, and challenges. Ongoing reports to the Presiding or Chief Judge on the COOP development progress helps maintain momentum and interest.

As part of developing the team, clear guidelines should be established to direct how the team will work together to create a COOP plan. By way of example, this may include a variety of items such as but not limited to the following:

- Establishment of a two-hour bimonthly meeting, establishing a schedule of when action items need to be completed.
- Establishment of protocols for use in case the Planning Team encounters resistance or can't obtain information.
- Establishment of protocols detailing how information will be stored and shared.

The COOP Planner should seek to involve and engage local emergency management officials (typically, these officials may reside in the County Sheriff, Fire, Risk Management, or other executive offices) to assist in plan development. Examples of the potential benefits of such connections and engagement include sharing of best practices and emergency management information resources, review of draft COOP plans, coordination of COOP plans with other government entities, sharing of training resources, and networking connections to the local

professional emergency management community. This may prove particularly helpful if a planner has been assigned to write the plan who does not have an emergency management background. More on working with local emergency management officials can be found in [Step 1-7: Meet with local/county emergency management](#).

STEP 1-4: REVIEW LEGAL AUTHORITY/RESPONSIBILITY IN COOP PLANNING AND ACTUAL DISASTERS

The COOP Planner should work with his or her court's Legal Counsel to understand any applicable state and/or local judicial emergency orders or rules regarding disasters or other emergencies. It is helpful to understand the laws/policies surrounding important issues such as suspending or extending statutes governing speedy trial provisions. Knowing this will be helpful when completing the essential function tables below (see [Step 2-6: Identify essential functions through a Business Impact Analysis \(BIA\)](#) and [Step 2-7: Conduct a Business Process Analysis on prioritized essential functions](#)). There will be a section within the table annotating any emergency regulations which provide relief on time-sensitive hearings/cases.

In many cases, these emergency orders or rules can help guide what will be considered essential court functions that need to continue and what legal relief a court of last resort can provide in a disaster.

STEP 1-5: GATHER INFORMATION ON PRIOR COOP PLANNING ACTIVITIES AND HISTORICAL LESSONS LEARNED

The COOP Planner should review any existing emergency plans currently in use or any that have been written in the past. Knowing what emergency protocols have already been developed will prove useful in developing the COOP. This can include plans such as Emergency Operations Plans/Occupant Emergency Plans, Evacuation Plans, and IT Disaster Recovery Plans. As a reminder, COOP is for significant emergencies that will impact operations typically over 24 hours. Many emergencies are short term in nature and may not necessitate activation of the COOP plan. A solid Emergency Operations Plan/Occupant Emergency Plan should be established to determine the policies and procedures dictating the response to short-term emergencies (e.g., fire alarm activation, bomb threat, medical emergency, or brief power outage). Many courts operate in mixed use courthouses. In these situations, all tenants of the building should operate off of a common set of emergency procedures to prevent conflicting guidance. Examples of other important pieces of information to be aware of include the following:

- **Previous disaster or emergency after-action reports.** If the court has experienced a disaster or an emergency situation in recent history, it is helpful to review past after-action reports, debriefs, or lessons learned. By learning how the court has responded to its past disasters, the court can better integrate those lessons learned into the COOP plan.
- **AOC COOP Plan guidance.** The COOP Planner will also want to assess if the State Administrative Office of the Courts (AOC) has any specific regulations or guidance pertaining to COOP. For example, is a COOP plan mandated by the AOC? Is there a format, template, or style that is mandated by the AOC?
- **Other projects and initiatives.** Other major projects and initiatives underway either internally or statewide could impact the development or implementation of the COOP plan (e.g., the use of video hearings, a new courthouse being built or decommissioned, a change in case management systems, or a new e-filing system). When writing the COOP plan, it is important to address how the plan may need to be modified due to any ongoing or planned projects or initiatives.

STEP 1-6: ACTIVATE THE COOP PLANNING TEAM AND SPECIFY PLANNING ASSUMPTIONS

Once the background work identified in Steps 1-1 through 1-5 is complete, it is time to engage the expertise and assistance of the COOP Planning Team. Before the COOP planning work begins in earnest and prior to the first COOP Planning Team meeting, it is helpful to provide some basic orientation so that all team members

understand the purpose of the COOP planning process. FEMA offers a basic one-hour online COOP Independent Study course ([IS-1300: Introduction to Continuity of Operations](#)) that provides an overview of what COOP is. As the planning team begins to meet, reviewing possible emergency scenarios is a good way to ensure the entire team is familiar with the potential complexities and challenges that can arise out of courthouse disasters or emergencies. Some examples of these include the following:

- Disruption to the operations of the court and/or courthouse may occur without warning and the COOP plan may have to be activated at any hour of the day or night.
- The physical infrastructure of court facilities may be compromised and the ability to continue to use the physical courthouse may be threatened or non-existent. Key infrastructure components and systems include the exterior envelope, structure, HVAC, power, water, and sewer.
- Once the COOP plan is activated, key personnel and the court's emergency organization may need to be moved to an alternate facility.
- The health and safety of employees may be at risk.
- Staff levels may be significantly reduced due to high levels of displacement, injury, illness, lack of transportation, and need to attend to family concerns.
- Remaining workers may be psychologically affected by disease, family concerns, concerns about economic loss, or fear, and require behavioral assistance.
- Some court functions (those deemed less vital) will have a lower priority and may need to be deferred until a later time.
- Information systems, communication, and transportation may not continue to function either unimpaired or at all; plans need to be activated almost immediately to compensate.
- There will likely be funding constraints.
- The geographical relocation of some or all the population may be extensive and/or may impact the resources available for recovery.
- Procurement of goods, services, and supplies may be impacted.
- Justice partners and other stakeholders will likely be impacted and their operational capacity may tangentially limit what the court can accomplish in an emergency.

A key takeaway from these scenarios is that each emergency or disaster brings unique complexities and issues. It is important to recognize the need for both careful planning and flexible response protocols that allow the court to maintain operations in challenging and dynamic situations.

STEP 1-7: MEET WITH LOCAL/COUNTY EMERGENCY MANAGEMENT AND KEY JUSTICE PARTNERS

Either the COOP Planner or the entire COOP Planning Team should convene meetings with the local and/or county emergency management agencies. This meetings can be used as an opportunity to define or clarify roles and responsibilities the court may have when interacting with its surrounding emergency management entity or entities.

The following is a list of questions that should be reviewed during this meeting. Many of these questions are relevant to specific components of the COOP plan and are referenced accordingly.

1. How does local emergency management envision the court's role in the local emergency response framework?
2. How can the court report operational status and resource requests to the local or county Emergency Operations Center (EOC)? (e.g., does the court have a seat at the EOC? If not, how are communication channels maintained?)
 - Information can be used in [Step 2-11: Define emergency communications](#)
3. What are the primary and alternate points of contact for court and Emergency Management entities?

- Information can be used in [Step 2-11: Define emergency communications](#)
- 4. Can the court have access to any web incident management systems the county is using (e.g., WebEOC)?
 - Information can be used in [Step 2-11: Define emergency communications](#)
- 5. Are there any grant opportunities available the court can take advantage of?
- 6. Are there any ongoing emergency management meetings or workgroups the court should participate in?
- 7. Where appropriate, how would the court apply for FEMA Public Assistance in a large disaster? Who would be the applicant? (Depending on facility ownership, this question may need to be coordinated with the State AOC as described in Step 1-8 below.)
 - Information can be used in [Step 2-19: Identify the cost recovery process](#)
- 8. Can emergency management help provide introductions or collaboration with local FEMA representatives or regional FEMA Continuity Managers?
- 9. Are there any training programs the court can participate in?
 - Information can be used in [Step 2-20: Training and Exercises](#)
- 10. How can the court be integrated into future local emergency management exercises?
 - Information can be used in [Step 2-20: Training and Exercises](#)

In addition, it will be critical to coordinate efforts with key justice partners (e.g., elected clerk of the court, public defender, prosecutor office, probation, etc.). It is important to determine how each stakeholder's COOP plan will mesh with the court's COOP plan to better ensure the overall resiliency of the community's justice system.

STEP 1-8: DEFINE THE ROLES/RESPONSIBILITIES BETWEEN THE COURT AND AOC

The COOP Planner or Planning Team should also consider convening meetings with State AOC representatives. Like meetings with local emergency management officials, these meetings can be used as an opportunity to define or clarify roles and responsibilities between the court and State AOC.

The following is a list of questions that should be reviewed during this meeting. Many of these questions are relevant to specific components of the COOP plan and are referenced accordingly.

1. How does the court apply for an emergency order from either the State AOC or court of last resort?
 - Applying for an emergency order from the State AOC/court of last resort will be an essential function. This information can be used in [Step 2-6: Identify Essential Functions through a Business Impact Analysis](#)
2. What support or resources can the State AOC provide to the court in an emergency?
 - Information can be used in [Step 2-13: Identify the resource management process](#)
3. How does a court's operational status get communicated to the State AOC? What type of information does the AOC need to obtain from a court during an emergency?
 - Information can be used in [Step 2-11: Define emergency communication](#)
4. How does the FEMA Public Assistance process work in the judiciary in a major disaster? What support or coordination do courts need to work with or through the AOC?
 - Information can be used in [Step 2-18: Identify the cost recovery process](#)
5. Will the AOC collaborate with the executive or legislative branch during an emergency? If so, how would this collaboration occur and what impact would it have on a local court?

SECTION II: WRITING THE PLAN

Section II covers the essential components of writing the COOP plan and is organized into the following parts:

- Part A: Readiness and preparedness
- Part B: Activating COOP in a disaster
- Part C: Ongoing COOP operations during emergencies
- Part D: Reconstitution and Cost Recovery

Section II includes a series of steps for the COOP Planner to follow in building a COOP plan. A detailed description of the purpose for each step and important COOP considerations related to each step are provided. As mentioned previously, users of this Guide are encouraged to make use of the tables presented as they work through the steps. These are the same tables as those included in the COOP Template located at the end of this document with one significant difference: the tables in Section II have been pre-populated with sample language based on a hypothetical court. The provided content can be used, where applicable and appropriate, as a starting point to facilitate the completion of the COOP Template. The completed template is the COOP plan! Hyperlinks allow the reader to “toggle” back and forth from the Section II tables to the template. **Therefore, users of this Guide can simply copy, toggle, and paste the information from Section II into the corresponding table in the COOP Template and then edit/complete as appropriate. This process is intended to assist COOP Planners in completing their own court COOP plans in an efficient, step by step manner.**

As mentioned previously, entering information in the COOP Template, in effect, constitutes writing the court’s COOP plan. In some cases, the pre-populated tables in this Guide may suit an individual court’s needs. However, COOP Planners using this Guide to build their own COOP plan should carefully assess if the pre-populated information included in the tables is appropriate and relevant for their specific court system. It is also important to note that although all of the steps in Section II are designed to build on one another, the COOP Planner may choose to proceed along the steps in any order that best suits his or her own court’s needs and planning efforts. The key is to make sure that, at the end of the process, all of the component parts included in this Guide have been addressed.

Some steps may be relatively simple to complete (e.g., [Step 2-5: Identify the court’s emergency operations center \(EOC\)/Meeting locations](#)), whereas other steps may require a great deal of planning and discussion (e.g., [Step 2-6: Identify the court’s essential functions](#) and [Step 2-7: Conduct a Business Process Analysis](#)). The pre-populated tables have been added to make the process of completing a COOP plan as painless and straightforward as possible; however, it must be pointed out that the process of completing a COOP plan is typically highly involving. Writing the plan as detailed in Section II will be the most time-consuming aspect of COOP planning covered in this Guide, but the effort put into it will prove to be extremely helpful in the future when the court faces a disaster or emergency.

PART A: READINESS AND PREPAREDNESS

STEP 2-1 DEFINE THE PURPOSE OF THE COOP

It is important that COOP plans have a purpose statement. This statement establishes a foundation of how the policies and guidance contained in the plan are relevant to the court in a disaster or emergency situation and sets the stage for how the court would respond in a continuity scenario. Table 2-1 below includes a sample purpose statement that may suit a court's needs.

Table 2-1: Purpose of the Court's COOP Plan

This COOP plan establishes policies and procedures to ensure the execution of essential functions for the court in the event that a disaster or emergency threatens or incapacitates operations. Specifically, this plan is designed to:

- Ensure that the court is prepared to respond to both natural and manmade disasters and emergencies, recover from them, and mitigate against their impacts.
- Ensure that the court is prepared to quickly transition from normal operations and maintain its essential functions in an environment where resources and facilities are threatened, diminished, or incapacitated.

[Link to Template](#) (Copy and paste the text from Table 2-1 above into the corresponding Table 2-1 in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-2: DEFINE THE PLAN'S APPLICABILITY AND SCOPE

This step describes what entities/individuals are covered by the plan and under what types of circumstances. Table 2-2 below includes a sample description that may suit a court's needs.

Table 2-2: Applicability and Scope

This plan applies to the (Court name) and its related facilities (specify name/locations). It covers all individuals who work or conduct business in these facilities. The plan takes an "all hazards" approach. That is, it applies to all emergencies, natural or manmade, that affect the essential operations of the court.

[Link to Template](#) (Copy and paste the text from Table 2-2 above into the corresponding Table 2-2 in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-3: DETERMINE THE DISTRIBUTION AND MAINTENANCE OF THE EXISTING COOP PLAN

In the case of an existing COOP plan, this step includes a place to note when revisions/audits of the plan were completed, what changes were made, and by whom. It is recommended that the plan be reviewed and updated annually. Below is an example of a completed revision control table.

Table 2-3A: Revision Control

Date	Summary of changes	By Whom
XX/XX/2021	Plan initially developed and approved	COOP Coordinator
XX/XX/2021	Essential functions updated to reflect new case management system	Chief Information Officer
<i>Insert others</i>		

[Link to Template](#) (Fill out Table 2-3A in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

The following Table 2-3B provides an example pertaining to the logistics of maintaining a newly completed or updated COOP plan. A COOP Coordinator should be identified who will be responsible for maintaining the COOP

plan. In most instances, this will be the same person (COOP Planner) who led the court’s efforts in developing its COOP Plan identified previously in Step 1-2.

Table 2-3B: Plan Maintenance	
Item to Consider	Response
Where will physical copies of the COOP plan be located?	Court Administrator Office, Facilities Office at all courthouses
Where will virtual copies of the COOP plan be located?	On the court’s internal emergency preparedness website.
Intended audience for this plan.	Executive Management, Chief and Supervising Judges, All Court Managers
Person responsible for maintaining the overall COOP plan.	COOP Coordinator
How often will this COOP plan be maintained?	Annually. Revisions must be approved by the [Presiding or Chief Judge] before [Day XX/Month XX]
Protocol for ensuring updates/revisions to this COOP plan are made for both physical and virtual versions.	COOP Coordinator will first update the electronic version on the court’s internal emergency preparedness site. COOP Coordinator will be responsible for updating the physical plan within three days of edits with the physical copy located in the Court Administrator’s Office. Local Facility Managers will be responsible for updating their local physical copy when instructed by the COOP Coordinator
<i>Insert others</i>	

[Link to Template](#) (Fill out Table 2-3B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-4: DEFINE THE CRISIS MANAGEMENT TEAM (CMT)

If the court already has an Emergency Operations Plan/Occupant Emergency Plan, a Crisis Management Team (CMT) may already be identified. If not, this is where the court will establish which staff and judges are needed to assemble in a crisis.

The CMT should function as an overarching policy/executive body that governs and directs policy related to crisis response for the court. In larger jurisdictions with multiple courthouses, there should also be some designation of Local Courthouse Unified Command Teams consisting of individuals who have crisis management responsibilities at the local courthouse level.

- **Policy Group** – Policy Group serves as a decision-making authority helping direct the priorities in an incident. This group decides major policy decisions such as closing a courthouse, deciding when to send Court staff home, determining court wide communication message, providing the court’s statement to the media, etc. The Policy Group should consist of the Presiding or Chief Judge, Chief Officers, General Counsel, Facilities Director, Public Information Officer, Emergency Management, and Lead Security Personnel (e.g., Sheriff Captain, Commander, etc.)
- **Local Court Unified Command Team** – A Unified Command Team will help direct incident response at their specific courthouse. They help provide quick emergency actions that take place at a single courthouse location. This team can consist of the senior judge at that courthouse, operations manager, facility manager, and local security lead. Ideally, this should be a small team (4-5 persons) but can expand to include other key management officials (e.g., jury services) as needed.

The CMT should include the COOP Coordinator. The COOP Coordinator will serve as the emergency management lead for the courthouse to help guide the court in implementing the COOP plan, serve as a liaison to external emergency management agencies, and help direct the court’s overall emergency management activities. As this position plays a key role, it is important to also identify a backup.

It is also helpful to consider additional supporting crisis teams that may need to assemble to work on specific functional issues. For example, an IT Crisis Team may be needed to provide support addressing IT

considerations for a disaster or emergency (e.g., expanding telework options, expanding videoconference hearings, addressing cybersecurity threats, etc.). The following Table 2-4 provides an example of a CMT worksheet.

Table 2-4: Crisis Management Team (CMT)	
CMT	Members of the Team
COOP Coordinator	Facilities Analyst
Backup COOP Coordinator	Facilities Specialist
Policy Group	Presiding or Chief Judge, Assistant Presiding or Chief Judge, Court Administrator, Operations Director, IT Director, HR Director, General Counsel, Public Information Officer, COOP Coordinator, Sheriff's Captain
Courthouse Unified Command Team – Juvenile Court	Juvenile Court Supervising Judge, Facility Manager, Juvenile Operations Manager, Sheriff's Sergeant.
Courthouse Unified Command Team – Criminal Court	Criminal Court Supervising Judge, Facility Manager, Criminal Operations Manager, Jury Manager, Sheriff's Sergeant
IT Crisis Team	Network Manager, End User Support Manager, CMS Application Manager, Cloud Applications Engineer
<i>Insert others</i>	

[Link to Template](#) (Fill out Table 2-4 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-5: IDENTIFY THE COURT'S EMERGENCY OPERATIONS CENTER

Knowing where the Crisis Management Team (CMT) members are to assemble in a disaster or emergency situation is critical. In traditional emergency management terms, the command center where emergency response is coordinated is often referred to as an Emergency Operations Center (EOC). Courts are encouraged to identify a centralized meeting place that will function as an EOC in the event of a disaster or emergency. This can help ensure the right people are gathering in the right location to make critical decisions. As disasters or emergencies can happen at any time during the day or night, it is helpful to explore both physical and virtual options. Table 2-5 below provides an example of a completed meeting locations worksheet.

Table 2-5: Meeting Locations		
Physical Meeting Options		
Courthouse	Inside Meeting Area	Outside Meeting Area
Policy Group – Primary EOC	Executive Conference Room on 2 nd Floor	Middle of judges parking lot
Downtown Courthouse – Unified Command Team	1 st Floor Training Room	Grassy area northwest of building
Juvenile Courthouse – Unified Command Team	3 rd Floor Conference Room	Center of plaza in front of courthouse
Virtual Meeting Options		
Virtual Modality	Protocols to Access	Any Restrictions
Microsoft Teams	Presiding or Chief Judge Assistant will email Policy Group with Teams meeting. Phone call instructions also to be included.	Can accommodate up to 250 users. All users must have either phone or internet connection.
External Conference Line	Presiding or Chief Judge Assistant will email Policy Group with dial-in instructions. Facilities Director and CIO have PIN and login access to open the line.	Can accommodate up to 60 callers at once. Phone line only. All users must have a working phone connection.

[Link to Template](#) (Fill out Table 2-5 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-6: IDENTIFY ESSENTIAL FUNCTIONS THROUGH A BUSINESS IMPACT ANALYSIS (BIA)

The core element of a COOP plan is the identification of a court's essential functions. These functions are fundamental to support the safety of the community, especially in times of crisis and with limited resources. Many essential court functions are determined by law, internal regulation or in a state or county-wide emergency preparedness meeting with justice partners. Essential functions are often linked to what is statutorily required of the courts. Other functions are judged essential based on criteria such as their importance to the court's mission, their role in the continuity of government, and/or their necessity to the performance of essential functions by other departments or agencies.

There are likely many other functions that are all very important but may not necessarily be "essential" in a disaster or emergency. Knowing what is truly essential and important to the safety and security of a community is vital. If essential functions are not clearly identified, it is easy for a court to become overwhelmed in a crisis, not knowing what is truly essential and what can be accomplished with limited resources. Thus, the mantra when selecting essential functions is: "If everything is important, then nothing is important." This step of the Guide is designed to help a court identify a list of its most time-critical and essential functions that cannot be left undone without running afoul of statutory obligation or risking failure of its mission.

Nailing down a court's essential functions is often the hardest part of COOP planning but one of the most critical elements of a COOP. Therefore, the COOP Planner and Planning Team may find that there is a considerable amount of work involved with completing Step 2-6 (and Step 2-7) as compared to the previous Steps 2-1 through 2-5.

Through the work completed under the first two initiatives of the SJI COOP grant as described earlier in this Guide, and as observed during the novel coronavirus pandemic in 2020, there are multiple case types that are typically prioritized during a disaster or emergency. Examples of these include the following:

- Criminal proceedings required to ensure due process of law and continuity of the criminal justice system.
- Domestic and civil proceedings required to meet the needs of the most vulnerable, such as those seeking protective orders.
- Probate proceedings required to resolve custody and property matters.
- Juvenile dependency and delinquency cases required to safeguard our youth even in times of crisis.
- Matters that arise because of the special circumstances of a disaster or emergency (e.g., hearings related to public health quarantine and isolation orders during a pandemic).

It is important to note that continuity of the court is not confined only to courtroom operations. It is critical to identify the administrative functions the court needs to operate. (e.g., payroll, payment to critical vendors, maintaining network connectivity, maintaining cybersecurity of court networks and databases, HR response to emergency leave requests, required building maintenance, collection payments, etc.).

A Business Impact Analysis (BIA) is typically performed within each department of the court to identify and prioritize essential functions. An essential function is defined as a court function that cannot be left undone for 30 days without risking failure of mission; failure to meet statutory/mandatory obligations; or loss of trust, respect, and funding. Each department should complete a business impact analysis and identify the specific essential functions needed to sustain critical court services. Court departments should also identify a Recovery Time Objective (RTO). An RTO is the amount of time within the department in which the process must be restored after an emergency event in order to avoid severe consequences. Once the department has a list of essential functions, each function should be prioritized as to its impact on returning to normal operations.

Table 2-6 below illustrates an example of a completed BIA worksheet. The worksheet should be used as a planning tool to determine and document what critical activities should be considered a true essential function. This activity may take several sessions to help define what is truly “essential.” BIA worksheets are often included as an attachment to the completed COOP plan. The department leads assigned to the COOP Planning Team would be responsible for completing these worksheets for their respective areas. The COOP Planner should ensure that all court departments have assessed their essential functions.

Table 2-6: Essential Functions - Business Impact Analysis Worksheet (COOP Plan Attachment)			
Department: Criminal Operations			
Critical Activity/Essential Function (EF)	Priority	Impact if EF is not completed	Return Time Objective
Process search warrants	High	Community at risk if warrants are not issued. Dangerous individuals may avoid capture.	24 hours
Criminal protective orders	High	Individuals at risk could be unprotected. Critical safety issue for those who need protection	24 hours
Criminal arraignments	High	Violation of a person’s statutory right to a speedy trial. In custody defendant could be released if not arraigned timely.	48 hours
Jury trials	Medium	Violation of a person’s statutory right if timelines are not relaxed by emergency order or rule.	1 week
Process payments	Low	Minor impact to court budget. Public can be held to certain judgments if payments are not posted. Court could issue local rule suspending judgments if payments can’t be processed to avoid impact to public.	1 week

[Link to Template](#) (Fill out Table 2-6 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

After each department completes their BIA, the COOP Planner and Planning Team should assemble and compile all BIA worksheets and prioritize all the essential functions on a court-wide basis. The compiled BIA allows the court to prioritize critical services and guides resource allocation. Presenting a compiled, prioritized list of essential functions to executive management and the Presiding or Chief Judge for their initial review can prove beneficial to ensure executive buy-in and support.

STEP 2-7: CONDUCT A BUSINESS PROCESS ANALYSIS (BPA) ON PRIORITIZED ESSENTIAL FUNCTIONS

After completing Step 2-6, the COOP Planner should now have prioritized lists of what each department considers as its essential functions. The next step is to identify the specific activities and processes that allow essential functions to be maintained during a disaster or emergency. This is where a Business Process Analysis (BPA) is helpful. The BPA is a systematic process that identifies and documents the activities and tasks that are associated with the court’s essential functions. The essential functions section of the plan should identify the resources, space requirements, costs, interdependencies, workflow processes, and support functions that ensure the continued execution of all the court’s essential functions. A BPA on each essential function should be conducted to determine the following:

- **Recovery Time Objective** – How quickly does this essential function need to come back online (e.g., one day, three days, one week, one month, etc.)? This information was already completed in Step 2-6 so information can be pulled from there.
- **Department/Person Responsible** – Which court department does this essential function fall under? In addition, which person will take the lead role to ensure the continuity of this essential function?

- **Key Staff/Personnel** – Who are the key staff/personnel needed to carry out this essential function?
- **Resources** – What are the necessary equipment and supplies to accomplish the essential function (e.g., court stamp/seal, laptops, etc.)?
- **Work Location and Space Requirements** – What specific layout or room is needed to accomplish the essential function?
- **Supporting Activities** – What are the activities that need to occur to ensure successful completion of the essential function (e.g., Facilities setup of a courtroom)?
- **Internal Dependencies/Essential Records** – What critical case management systems, computer programs, databases, bank routing numbers, etc., are needed to accomplish this essential function?
- **External Dependencies/Essential Records** – What external justice partner IT applications/programs or services are needed to accomplish this essential function? (e.g., DMV interface, credit card processing system, criminal complaint from prosecutor’s office)
- **Manual Workarounds** – Are there manual workarounds developed in the event critical IT systems supporting the essential function are not available?
- **Judicial Emergency Orders** – Can emergency orders from the State's court of last resort provide any assistance to suspend deadlines or extend timeframes for accomplishing the essential function?
- **Related Regulation** – What requires the court to perform the essential function? Cite the government section or penal code reference if known.
- **Telework** – Can the essential function be conducted remotely?

Completing the BPA provides context and key information to help management continue essential functions in a disaster or emergency. A BPA will help the court understand the complexities and interdependencies needed when a disaster or emergency occurs. As the court will most likely have many BPA tables (one for each essential function), it may be helpful to organize them via department and/or case type to help with easy retrieval during a crisis. The court may also consider integrating this information into an Excel workbook or other data analysis tool to help with organizing, filtering, and sorting of information.

The following Table 2-7 is a court-centric version of the Essential Function worksheet included in the [FEMA Continuity Plan Template and Instructions for Non-Federal Entities and Community-Based Organizations](#).

Table 2-7: Essential Functions (EFs) - Business Process Analysis

Essential Function	Recovery Time Objective	Department/Person Responsible	Key Staff
Conduct criminal arraignments	24 hours	Criminal Operations/Criminal Manager	1 Judge, 2 Clerks, 1 Court Reporter, 1 Interpreter per courtroom. Total of three courtrooms needed. 1 Criminal Operations Supervisor to oversee operations.
	Resources Needed		
	Court seal, US and State Flag, court stamps, judicial robe, headsets for interpreters.		
	Work Location & Space Requirements		
	Three courtroom sized spaces. 1-2 judicial chambers (can be shared between three judges), secure passageway and holding area for in custody inmates.		
	Supporting Activities		
	Receive criminal filing from prosecutor's office. Have in-custody inmate transported to courtroom.		
	Internal Dependencies/Essential Records		
	Criminal Case Management System. Warrant Tracking System.		
	External Dependencies/Essential Records		
	Criminal complaint from prosecutor's office. Sheriff bailiff services. DMV records. State law enforcement database.		
	Manual Workarounds		
	Will need to manually receive complaint from prosecutor's office. Use manual criminal operations forms if case management system is non-operational.		
	Related Regulation		
	Government Section Code: 285b		
Can an Emergency Order provide relief?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Notes: EO from the court of last resort can provide relief to extend timeframe up to 14 more days.		
Can EF be done via telework?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Notes: Not readily feasible unless remote appearance can be accomplished at jail.		

[Link to Template](#) (Fill out Table 2-7 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Ultimately the final COOP plan describes how all the required resources will be allocated during a disaster or emergency to ensure that essential functions can be maintained. The administrative, technological, legal, and human resources aspects of these resources allocated during the disaster or emergency should be considered, e.g., purchase orders, agreements with companies, technology protocols, communication plans, legal requirements, and HR considerations.

STEP 2-8: EXPLORE TECHNOLOGY CONSIDERATIONS – ESSENTIAL RECORDS, COURT APPLICATIONS, NETWORK

Court technology is often considered the backbone of maintaining the continued administration of justice. The process of prioritizing critical court technology elements and identifying what essential functions they support will be important to determine prior to a continuity event. Thus, this step should be done somewhat concurrently when developing an essential functions list (Step 2-6 and 2-7). Some of the questions listed when conducting a business process analysis for the court's essential functions are directly related to this Step 2-8. When considering the essential function list, often there are critical IT elements that are needed to successfully execute an essential function (e.g., case management system, imaging systems). These are often referenced as either internal or external dependencies. Ranking those applications with their recovery time objective will assist the IT department in knowing what the priority restorations are and where to divert limited resources during a crisis. For example,

only the applications that support the essential functions are ranked and considered critical, other applications are ranked lower with return times set after the critical applications are restored.

Planners must also consider the sequencing of how these steps come back online. If, for example, a case management system needs to be restored, servers and internet access will first need to be restored. Thus, the order of restoration is a key determining factor when evaluating how quickly technology needs to be brought back online. The order of restoration of systems should be considered for all critical software applications and infrastructure (e.g., email, phones, servers, etc.). An IT Recovery Time Objective (RTO) identifies the maximum amount of time that IT systems can be down before severe consequences are experienced. The important question for the court to answer is how long it can afford to be in the dark?

Another important metric in managing expectations in recovery efforts is defining a Recovery Point Objective (RPO). If IT services are interrupted before backups are updated, some data loss can occur. The RPO establishes the maximum age of the files recovered from backup storage that are necessary for operations to resume. For example, if the RPO is 24 hours, backups should be made at least once per day. This means that, in the event of a disaster, the court would potentially lose up to one days’ worth of data.

In addition to IT applications and infrastructure, it is critical that consideration be given to the essential records necessary to continue essential functions in the event of a disaster or emergency. Examples include emergency plans, manual workaround procedures, legal and financial records, property management records, procurement agreements, inventory records, payroll rosters, next-of-kin notification, etc.

The following Table 2-8A will help prioritize and identify IT applications and essential records that were identified when developing an essential function list.

IT Application/Vital Record	IT Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Unit Responsible/Point of Contact	Notes
Email	1 hour	24 hours prior	Cloud Applications Unit, Cloud Application Manager	Microsoft 365 cloud-based solution
Servers	1 hour	72 hours prior	Infrastructure Unit, Infrastructure Manager	Majority of servers are in Criminal courthouse
Criminal case management system	24 hours	72 hours prior	IT Application Unit, Application Manager	Cloud based
VOIP Phones	48 hours	N/A		
Protective order database	48 hours	1 week prior	Criminal Operations, Criminal Manager	Relies on physical server at downtown courthouse
Payroll Information	1 week	1 month prior	Accounting, Accounting Manger	County maintains backup of court payroll for one pay period (two weeks)

[Link to Template](#) (Fill out Table 2-8A in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

The strategy for ensuring the integrity of essential records may vary depending on the data systems in place. FEMA has provided guidance on several options for ensuring access to essential records during an emergency. These include:

- **Using backup servers.** Data and records are backed up on a secondary server, in addition to the primary server. When the backup server is stored in a different location than the primary facility, an organization increases the possibility that data and records are available and accessible.

- **Pre-positioning hard copy records.** Printing hard copy records ensures an organization is not reliant on electronic equipment to access records. Prepositioning copies at alternate operating locations further protects an organization should the primary facility become inaccessible.
- **Leveraging cloud computing.** In cloud computing, remote servers hosted on the Internet are used to store, manage, and process data. This disperses risk to an organization as data is not hosted on local servers, provided that the cloud service provider also has adequate continuity plans.

The COOP plan should cover how essential records and applications are maintained, how they are backed up, and how they can be accessed in an emergency. If operations need to be taken offsite, there should be a discussion of how staff/judicial officers at offsite locations can access these essential records and applications. Some external records may be restricted from being accessed anywhere else but a courthouse.

The work being done in this step of the COOP plan is only a very small part of the work needed to prepare IT departments for disasters. With the increasing reliance on technology and the emergence of cybersecurity threats, it is critical that courts also consider developing a full IT Disaster Recovery plan separate from the COOP plan. An IT Disaster Recovery plan will provide much greater detailed protocols for networks/application backups and restoration, and will specify the mitigation measures needed to protect a court's IT infrastructure. The IT Disaster Recovery plan should include a process by which all essential functions can be executed in the event that IT systems are not available and a process by which essential functions and essential records are maintained and reintegrated into networks/applications once systems are restored. The technical expertise required to complete an IT Disaster Recovery plan usually dictates that it be prepared under a court's IT department and will typically fall outside the scope of the base COOP plan described in this Guide; however, the information contained within the IT Disaster Recovery plan will be critical in a crisis.

Telework considerations – Telework may be a critical tool in maintaining the court's essential functions during an incident. When developing essential functions and the key requirements for executing them, it is helpful to consider if telework can be utilized.

The following Table 2-8B provides an example of telework considerations.

Table 2-8B: Telework Logistics

Item to Consider	Explanation, Response, or Protocol
How many telework (VPN) licenses does the Court maintain?	200
Does the court have a current policy on how telework will be used in a crisis?	Yes – Telework Policy #XX-XX, developed during the COVID-19 pandemic, defines who can telework and its parameters. When COOP is activated, this policy is in full effect.
What IT cybersecurity protocols need to be in place to implement emergency telework?	All court issued computers have appropriate network security protocols and applications in place. If staff are using their own computers to connect remotely, those personal computers must have updated antivirus software and their home Wi-Fi must be password enabled. Policy #XX-XX addresses these specific requirements.
What will be the plan to surge telework options (e.g., purchase new laptops, reuse existing computers)?	All those who are issued laptops will be required to take them home. If possible, those authorized for telework will schedule a time with IT to take their entire desktop computer home (if feasible). The court can also utilize a state master agreement through the AOC to purchase laptops in an emergency.
What changes need to be made to the court network or infrastructure to support expanded telework?	IT will monitor bandwidth traffic and work with our internet vendor (insert vendor name) to determine if bandwidth needs to improve. There will be a weekly audit by the IT Infrastructure Manager to the Court CIO to assess bandwidth and any changes. If hearings are being done virtually and sessions are live-streamed, bandwidth will need to be increased by at least 25%.
How will telework capabilities be tested prior to an emergency	Those who are assigned court laptops are asked to take them home, turn them on, and connect to applications related to their applicable essential functions. This test is done two times per year (June and December). All employees who are authorized to remote work should remote login at least twice a year to ensure their two-factor authentication is set up correctly.
How will telework equipment be deployed to judges/staff?	All equipment will be distributed from the main courthouse. IT has a stockpile of IT supplies at this location. Peripherals (mice, monitors, keyboards, etc.) can be taken from other courthouses if needed but distribution will occur at the main courthouse. The Juvenile courthouse will serve as a backup in the event the downtown courthouse is not accessible.
How is bandwidth addressed for critical applications to be used offsite or at an alternate facility?	IT maintains ten hotspots (List vendors). These hotspots will be taken to any offsite/alternate facility where emergency court operations may be established. IT Infrastructure would be responsible for conducting these tests and working with Court Operations to determine the needed bandwidth for applications based on the number of judges/staff assigned to the facility.
Are there any court applications, software, or programs that can't be accessed offsite?	The DMV application can't be accessed offsite. Special provisions can be made in a presidentially declared disaster but must be submitted in writing to the DMV IT office.
What type of ergonomic protocols need to be in place for telework to prevent injuries?	When telework is authorized in an emergency, HR will include a one-page information sheet on how to maintain an ergonomic workspace at home. HR will remind workers on key steps they can take to prevent repetitive motion injuries and how they can stay safe at home. Staff will be reminded that if they do experience an ergonomic injury, they need to report it to their supervisor and HR since worker's compensation packets will need to be sent to the employee working remotely.
How will employee privacy be maintained during telework?	Employees will be given Google Voice numbers. No personal cell phone information will be released to the public.

[Link to Template](#) (Fill out Table 2-8B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

As a reminder, low-tech solutions can also help courts deal with the disruption of IT systems in the event of a natural disaster. During significant natural disasters, courts may have to implement manual paper processes. Although much progress has been made with e-filing and “going paperless,” retaining paper copies can be beneficial during disasters. In situations where a disaster requires the implementation of manual processes, it is also important to plan for the transition from temporary manual processes back to the automated electronic processes during the recovery. This will help set expectations for time and resource allocation during recovery. The table described in Step 2-7 above ([Table 2-7: Essential Functions - Business Process Analysis](#)) includes a section that discusses what manual workarounds are available to fulfill essential functions in the event that the technology needed is not available.

STEP 2-9: IDENTIFY ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

Disasters can potentially impact the ability of key judges/staff to report to the courthouse to fulfill their responsibilities. As such, it is important to identify successors for key positions as well as what authority will be delegated to them during the crisis.

Orders of Succession provide for the orderly and predefined assumption of authority and responsibility during a disaster or emergency in the event that court leadership officials are unavailable to execute their duties. Successors should be identified for at least the CMT, Executive Management, Judicial Leadership, and Directors of all court departments. The number of key decision-makers will be dependent on the size of the court and its management structure. Ideally, courts should identify three successors for every key decision-maker; however, this may not be realistic for smaller courts. When possible, it is helpful to identify at least one successor who works in a different location than the key decision-maker and other named successors.

Delegation of Authority – Delegation of authority is the process of transferring responsibility for a task to another employee during a crisis. In most cases, a successor will assume the authority to perform all functions that the position performs under normal operations. However, for some successors, the authority to perform certain functions may be limited. For example, if an assistant accountant is designated as the court’s third successor for the Finance Director, the planning team may decide to limit the assistant accountant’s authority for expenditures to a certain amount. The successor would need to obtain permission from the Court Administrator and Presiding or Chief Judge to authorize expenditures over that designated amount. It is also important to identify when a successor’s authority is activated and when it is terminated. When considering succession planning, a court should consider if the successor has the tools and resources to complete that job function. Therefore, the plan should address what types of physical/IT/essential record access may need to be modified when a successor assumes their position.

Table 2-9 below provides an example of defining successors, their delegated authority, timeframes of their authority, and what resources might be needed.

Key Position	Successor	Delegated Authority	Activation/Termination of Delegated Authority(s)	Resources Needed
Chief Finance Officer (CFO)	Financial Planning Officer	All with one exception: Any purchases above \$25,000 need to be approved by the Presiding or Chief Judge.	Activated: CFO is not available during COOP plan activation. Terminated: CFO is available, or emergency is over.	Court Credit Card.
	Accounting Manager	All with two exceptions: One is any purchases above \$25,000 need to be approved by the Presiding or Chief Judge. Second, person does not have the authority to hire/fire finance staff.	Activated: Financial Planning Officer is not available during COOP plan activation. Terminated: Financial Planning Officer is available, or emergency is over.	Court Credit Card. Access to Level 4 authority in purchasing system.
	Collections Manager	All with two exceptions: One is any purchases above \$25,000 need to be approved by the Presiding or Chief Judge. Second, person does not have the authority to hire/fire finance staff.	Activated: Accounting Manager is not available during COOP plan activation. Terminated: Accounting Manager is available or emergency is over.	Court Credit Card. Access to Level 4 authority in the purchasing system.

[Link to Template](#) (Fill out Table 2-9 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-10: IDENTIFY ALTERNATE FACILITIES AND GO KITS

Not all disasters will impact courthouse facilities. However, the court must be prepared to continue essential functions in alternate locations to ensure the continued administration of justice. Often, alternate facilities are not a traditional courthouse. It is important to prioritize essential functions before considering alternate facilities so the court is aware of what essential functions must resume at an offsite facility if needed. When considering alternate facilities, it is helpful to identify who will take the lead in the event an alternate facility needs to be identified and set up. It is important that the IT department is part of any alternate facilities discussions during both the planning and implementation stages. Network access, bandwidth capabilities, and access to critical case management systems and databases are all critical elements needed to successfully create a functional alternate facility.

Due to the unique challenges and configurations of courthouses and courtrooms, it is advisable for courts to investigate the possibility of moving operations to another existing courthouse before considering external alternate facilities. Identifying how existing courthouses could absorb critical essential functions in the event a courthouse becomes unusable can prove highly beneficial given the unique facility needs for conducting court operations.

It is helpful to consider alternate facilities from the perspective of a court user. A disaster or other emergency may require court services to be provided in different locations or buildings, which in some cases may not be a traditional courthouse. It is important to ensure that public access issues are addressed, such as informing the public how and where services may be accessed. Key questions to consider include:

- How will visitors know where to go?
- Where will visitors park?
- Is the alternate facility universally accessible for persons with disabilities?
- Is there appropriate signage and is that signage available in multiple languages?
- Can staff assist in guiding court users where to go?

A best practice in emergency management is to have a “hot site” available where it is move-in ready with the necessary IT, furniture, configuration, security, etc., but that is not a reality for most courts due to the ongoing financial burdens. Thus, considering partnerships with other government entities, federal courts, surrounding court systems, universities, law schools, convention centers, hotels, and the like can prove beneficial. Courts should explore creating Memorandums of Understanding (MOUs) to assist in this (FEMA provides a sample MOU agreement that can be utilized, which can be found on page 42 of the [FEMA COOP Template](#)). Partnerships with local emergency management to identify space options can also be helpful.

The following Table 2-10A illustrates a sample completed checklist of court specific considerations related to the identification and evaluation of alternate facilities. Completed checklists can be included as an attachment to the court’s COOP plan for later reference.

Table 2-10A: Alternate Facility Evaluation Checklist
(COOP Plan Attachment)

Alternate Facility Criteria	Comments
Physical Layout	
Where is the facility located?	University Law School
How much floor space does the facility have?	6,000 sq/ft total broken up into four large rooms of 1,500 sq/ft
Can the rooms be partitioned? Is the available floor space contiguous or on different floors/in different wings?	Yes. Rooms are all contiguous.
How many staff workstations can the facility accommodate?	Each room can accommodate at least 10 workstations or one functional courtroom.
How many courtrooms can the facility accommodate?	4
Does the facility have electricity, backup generator, and available power outlets?	No backup generator but plenty of wall outlets.
Does the facility have desks, chairs, and other furniture needed for setup?	Yes. As It is a school, there are already desks/chairs inside the facility.
Are any private offices available? Any rooms that could be used as judicial chambers?	None
Are there break rooms available for staff?	2 nd Floor of the Law School has a student study area that could be converted into a break room.
Are restrooms available for the public, staff, and judges?	Yes.
Is there available parking for staff and the public?	Yes. Paid parking at \$5/day.
How easy is it for the public to find the building? Is the building ADA accessible?	Very easy. Existing signage works to identify building.
Is the site best suited for courtrooms, case processing, office work, public counter services, etc.?	Courtrooms and workstations. No counter services could be conducted here.
What type of agreement (e.g., financial contract, memorandum of understanding/agreement, statutory change to allow the court to sit in another jurisdiction) is necessary to secure the facility for the court's use?	Court will need an MOU.
IT Functionality	
Is the facility equipped for internet or wireless internet connectivity? Is the signal strength strong enough to support the needed IT applications?	Yes. University can offer a VLAN for hardwired connection. Signal strength is strong (100mbs download speed).
If using mobile hotspots, what is their signal strength? Is the signal strength strong enough to support the needed IT applications?	AT&T – XX mbs, Verizon – XX mbs. Signal strength is adequate for a single courtroom with 4 computers using the criminal case management system.
What critical IT applications need to be accessed from the facility?	Criminal Case Management System.
What type of phone lines are available?	No phone lines available. Cell phones will be needed.
Security Considerations	
Are there secure areas to lock sensitive or confidential items after hours?	Yes. Second floor has a secure faculty area with a locking closet the court could use.
Is there a secure parking area and entry for judges?	No.
Are there any security vulnerabilities? (e.g., multiple entrances, no escape for judge/staff)	Due to university environment, there are multiple entrances/exits to the facility.
If inmates are to be transported to the facility for hearings, what type of secure access will there be to get them in/out of the facility?	Facility is not suitable for inmate movement.
How much security personnel will the facility require?	9 security officers to provide bailiff and weapons screening services (includes relief).
Is there a location for a weapons screening station to be set up?	Yes. Main lobby on the 1 st Floor has enough space.

[Link to Template](#) (Fill out Table 2-10A in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

The following Table 2-10B can be used to record key information pertaining to alternate facilities once those facilities have been identified. Additional information needed for activation of may be referenced from completed checklists in Table 2-10A above.

Table 2-10B: Alternate Facility Locations

Alternate Facility #1 Facility name: Community College Address: 23 Main Street, Anytown USA Point of Contact: Dean John Doe, (310) 111-2222, johndoe@court.gov	
Expected Use (courtroom, offices, jury assembly, etc.)	Three classrooms can be used for civil protective order courtrooms. Six offices are available for judges, clerks and admin staff. The gymnasium can be used for jury assembly.
Available Utilities	Power, HVAC, Water all available. Classrooms on generator power.
Furniture/Equipment Needed	University can only provide tables and chairs. All other items to be provided by the court.
Wi-Fi/Network Options	Wi-Fi signal good with Verizon and AT&T hotspots (above 20mbs download). University can offer VLAN option
Floor space (sq./ft)	Classrooms are 1,500 sq./ft. Gymnasium is 10,000 sq./ft.
Parking Availability	Parking is plentiful, but users will need to pay daily rate of \$5/car.
Accessibility Concerns	Wheelchair-bound visitors will need to be escorted through the side door.
Vulnerabilities	No secure judicial parking; lacks separate entrance for judicial officers
Agreement	MOU signed on XX/XX/2021 and stored in the Contracts database.
Staffing Considerations	
List potential anticipated number of judges and staff reporting to the alternate facility	Three judges, nine court clerks, one civil manager
Who is responsible for judges/staff reporting to the alternate facility?	Manager in charge of that operational unit
Who provides orientation on the following topics? (break room, restrooms, parking, security, safety, emergency evacuation, supplies, card/key access)	Local facility manager
Who provides notification to the following entities about the alternate facility?	
Staff	Manager in charge of that operational unit
Parties/Litigants	Clerk's Office
Justice Partners	Manager in charge of that operational unit
Public	Court Public Information Officer
Alternate Facility #2 (Add additional facilities as appropriate)	

[Link to Template](#) (Fill out Table 2-10B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Go Kits – When relocating to an alternate facility, the court will most likely need to transport necessary supplies to ensure the continuation of that essential function. Court departments should develop “Go Kits” in advance to ensure the continuation of their specific essential functions.

Each court department should have one or multiple Go Kits in the event a court department must relocate quickly. These kits help ensure the court can continue its essential functions if asked to relocate to a different facility. These kits only contain items that are vital to the performance of the department’s essential functions. A kit may include a USB drive to include important documents such as manuals, forms, contacts, and links necessary to perform essential functions, even if this data is hosted on a cloud site. The kit may also include a physical box or bag with manuals, supplies, equipment, etc. that are necessary to perform a department’s essential functions. As stated earlier, one should not rely on the presence of technology and should always consider a manual work around to execute essential functions.

‘Pre-Staged’ vs. ‘To Be Recovered’ – One suggestion to ease the financial burden of purchasing numerous items for Go Kits is to consider the concepts of ‘pre-staged’ and ‘to be recovered’. When considering Go Kits, court management must balance cost versus preparedness. There are numerous items that can be easily purchased or pulled to be ‘pre-staged’ inside a Go Kit. These ‘pre-staged’ items include forms, documents, basic office supplies, etc. There are also high-value items (e.g., laptops, printers, scanners, etc.) or items that require frequent updates. It may not be fiscally viable to purchase these high-value items for emergency use only. As such, one option is to have managers designate high-value items as ‘To Be Recovered.’ When a COOP event occurs, the hope is that managers will have access to the courthouse just long enough to recover these items from existing stock to be used at another location.

Below are some key considerations when evaluating Go Kits:

- **Number and Location:** Court management will need to determine (based on their essential functions) if a single Go Kit can serve the unit or if multiple Go Kits are needed at each facility.
- **Security and Accessibility:** Go Kits should be securely stored but also must remain readily available in an emergency. They should not be locked in an individual’s cabinet as access could be problematic in a real incident. However, these items should be stored in a secure area to prevent theft or employees using these items for day-to-day use.
- **Maintenance:** Go Kits should be maintained and inspected annually to ensure they are still applicable and readily deployable.
- **Suggested items:** Each department’s Go Kit will be unique to the essential functions it must carry out.

Below are some suggested items to include in the Go Kit:

- Documents, forms, and guides
- Manual forms and procedures
- List of critical websites (internal/external)
- Electronic storage media (e.g., USB) containing applicable documents
- Basic office supplies (e.g., post its, writing pads, stapler, pens, envelopes, receipt books, etc.)
- Carrying case or backpack

The following Table 2-10C is an example of a Go Kit checklist that can be created. Completed Go Kit checklists can be included as an attachment to the court’s COOP plan.

Table 2-10C: Go Kit Checklist
(COOP Plan Attachment)

Go Kit (Department/Unit)	Facilities Team		
Go Kit Location	Downtown courthouse 1 st Floor (backpack near Facilities entrance)		
Last Checked	01/15/2021		
Item	Pre-Staged	To Be Recovered	
Mass Notification Cheat Sheet (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Card Access Cheat Sheet (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Contact list of emergency vendors (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Facility maps for all facilities (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Asbestos surveys (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Courtroom information sheet (printed)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
USB device containing above items	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(3) Laptops and charging cables	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Keys to court vehicles	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
(3) Hardhats, safety goggles, gloves	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(3) Court emergency radios with chargers	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
(3) Flashlights	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Tape Measure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(3) Writing pads with clipboards	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Pens (writing and sharpies)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(3) Gaffers Tape	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(5) Surge protectors and extension cords	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(3) Moving Dollies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Portable generator with spare fuel	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

[Link to Template](#) (Copy and paste the text from Table 2-10C above into the corresponding Table 2-10C in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-11: DEFINE EMERGENCY COMMUNICATIONS

There are three key areas of communication the court must consider during a disaster or emergency:

1. Communications to **inform court judges/staff** about the status of the court in addition to their roles and responsibilities during an incident; and
2. Communications to **advise justice partners and other government entities** of the court’s operational status and coordinate services and resource requests; and
3. Communications to **advise the public** about the court’s operational status and the status of individual court cases.

The court should identify all available modalities of communications that can be used during a crisis. Ideally, a mix of redundant modalities should be considered so the court does not become overly dependent on just one or two forms of communication. Day to day modalities such as email and phone can certainly be utilized but it is helpful to review other communication options for use in a disaster or emergency situation. A sample of these different options include the following:

- Mass notification systems (Typically these are third party systems which provide rapid alerting to many individuals through a simultaneous email, phone call, and text message. These systems are a way to quickly contact many individuals and take the place of older phone trees.)
- Court website

- Emergency phone message number (Number where judges/staff can call in to obtain recorded updates about the court's operational status.)
- Cloud based websites (Location where judges/staff can obtain information offsite in the event they cannot access the court's network.)
- Emergency conference lines (internal/external)
- Two-way radios (Confer with the local sheriff and/or emergency management office to see if they can provide recommendations on frequencies or radio infrastructure.)
- Satellite phones
- Videoconference platforms
- Social media
- External facility signage
- Fax lines
- Building public address (PA) systems

In addition, the court should explore priority communication services reserved for government entities to maintain continuity of critical services. The following are a few examples the court could explore as judicial branch entities are eligible to receive these services. Some come with recurring costs while others are available at no cost.

- **GETS** – Courts can register for the [Government Emergency Telecommunications Service \(GETS\)](#), a free program of the Department of Homeland Security's Office of Emergency Communications. GETS is intended to be used in an emergency when the landline network is congested. It provides priority access and processing in landline networks and increases probability of call completion. This service is provided at no cost to the court.
- **WPS** - The [Wireless Priority Service \(WPS\)](#) is a Federal program that authorizes cellular communications service providers to prioritize calls over wireless networks. Participating service providers typically deploy WPS in stages, beginning with top priority entities, until service is available in most coverage areas and functionality has reached full operating capability. This service is also provided at no cost to the court.
- **Mobile Telecom Provider Priority Network** - (e.g., [Verizon First Responder Network, FirstNet](#)) - A newly introduced emergency communications network for courts to consider includes the First Responder Network Authority ("FirstNet"), an independent authority established by Congress which will deliver a dedicated nationwide broadband network (Band 14) to emergency service providers. There may be nominal charges for courts to access the FirstNet equipment and network.

Table 2-11A on the following page denotes how to capture all the various communication modalities that can be used in an emergency and how those modalities will be used.

Table 2-11A: Communication Modalities

Communication System	Where is system located?	Who has access?	Unit responsible?	Who can receive communications?
Voice Lines	All workstations and courtrooms	All	N/A – all judges/staff have access to use phones	All judges/staff
Email	All workstations and courtrooms	All	N/A – all judges/staff have access to email	All judges/staff
Mobile Phones	Executive Management are issued Verizon mobile phones	Executive Management Only	Facilities department responsible for maintaining mobile phone contract	No restrictions on where calls can go to. Phones can be used as mobile hotspots if needed.
Mass Communication (ReadyCourt)	Cloud based system	COOP Coordinator, Court Administrator, HR Dir., Facility Dir.	COOP Coordinator oversees contract with third party vendor.	All judges/staff. Some key stakeholders (e.g., prosecutor, public defender, probation).
Two-Way Radios	Evacuation leaders at all courthouses and CMT	Evacuation leaders at all courthouses and CMT.	COOP Coordinator	Only those who have a radio (Court uses Channel 1, Sheriff uses Channel 2).
Emergency Phone Message Number	Hosted on the VOIP server (number is XXX-XXX-XXXX)		COOP Coordinator or HR Director can leave messages on this line.	All judges/staff
Cloud based information site	Secure online SharePoint site https://secure...	IT Director, COOP Coordinator, HR Director	COOP Coordinator will post updates on at the direction of the CMT	All judges/staff
Videoconference Platforms	Microsoft Teams, Cisco WebEx	All judges/staff	IT Director	All judges/staff
Satellite Phones	One phone located at each courthouse in the Facilities Office	Facility Manager	IT Director	No restrictions on where calls can go to.
Social Media	Facebook, Twitter	PIO	PIO	Public access
GETS/WPS	All CMT members are issued GETS cards and have WPS on their court mobile phones	All CMT members	COOP Coordinator	GETS works on landline networks and can dial all numbers. WPS will give priority on mobile phones.
FirstNet Devices	One FirstNet phone located at each courthouse	Facility Manager	IT Director	No restrictions on where calls can go to. Phones can be used as mobile hotspots if needed.
Fax Lines	One fax located in the facilities department in every courthouse. Fax numbers stored on SharePoint site	All judges/staff	Facility Managers	Any available fax lines.
Building PA systems	Downtown and Juvenile courthouse have building wide PA systems	Facility Manager and Sheriff Staff. Messages sent from local control station.	Facility Manager	All building occupants in the Downtown and Juvenile courthouse.
<i>Insert others</i>				

[Link to Template](#) (Fill out Table 2-11A in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

After identifying all the various modalities that the court can use, a communication strategy should be developed which includes the following:

- Protocols for situational awareness

- Communications with stakeholders and partners
- Last resort communications plan

A key element when considering protocols for situational awareness during an emergency is the development of a Common Operating Picture (COP). COP can be a tool that provides situational awareness allowing court officials to make accurate, informed decisions based on current or planned activities during an emergency incident. Data and real time sources used to support all court functions in a response are displayed onto a single platform. This platform can be as simple as a whiteboard that highlights key decisions, messages, actions, etc. inside a conference room where the CMT meets, or complex cloud-based tools (e.g., WebEOC) where court departments can electronically upload situation updates into a real-time virtual platform/chat room.

Communications with stakeholders and partners are critical during a disaster or emergency situation. The court should determine who will provide such communications to each stakeholder and partner, and at what frequency. Setting up regular situation status briefings with the CMT and key management/stakeholders helps develop the court’s COOP plan. A sample situation status briefing agenda is shown below.

Sample Situation Status Briefing Agenda

Topic 1: Emergency Management and Executive Opening

- *COOP Coordinator provides situation assessment*
- *Presiding or Chief Judge and/or Court Administrator Concerns and Priorities*

Topic 2: Departmental Reports on Impact of Disaster and Current Response Efforts

- *Facilities*
- *Operations – Review all case types*
- *General Counsel*
- *HR*
- *IT*
- *Finance*
- *Security*

Topic 3: Contingency Planning

- *Review what contingency plans have been developed*

Topic 4: Communication – Assess what communication has been sent or needs to be sent to the following stakeholders:

- *Judges/staff*
- *Jurors*
- *Justice Partners and Building Tenants*
- *Media/Rumor Control*
- *Public – verbal, physical signage, social media, website*
- *Local emergency management agency*
- *State AOC*

Topic 5: Resources

- *Assess any gaps in current resources/supplies*
- *Assess what resources need to be procured*

Topic 6: Determine when next briefing will occur

Lastly, even with multiple redundancies, it is helpful to identify a “last resort” plan of communication. If all technology is down, how will the CMT communicate with one another and with court judges/staff? The following Table 2-11B denotes a communication strategy for how the court will communicate with its stakeholders and partners.

Table 2-11B: Communication Strategies

Protocols for Situational Awareness

How will the court maintain a Common Operating Picture (COP), so management and judicial leadership understand the situation and what the operational plan is?	COOP Coordinator will schedule regular (daily or weekly depending on incident) situation status briefings with the CMT. In addition, the court maintains a cloud-based SharePoint site (Court WebEOC) where managers across all court departments will post a daily update.
How will the court provide updates to judges/staff who may not be onsite or have access to their court email?	The court will activate its cloud-based SharePoint site (Court Emergency Page). Alerts will be sent via the mass communication system (Ready Court) to all judges/staff when updates are made to this site.
How will the court communicate operational status to the local/county emergency operations center?	The COOP Coordinator is on the activation roster for when the County EOC activates and thus will participate in all ongoing conference calls. COOP Coordinator also has a login to the County's WebEOC portal thereby allowing the court to share situation status to the County EOC. The County EOC Director will serve as primary contact with the court. The backup contact will be the northwest regional Emergency Management Specialist.
Does the court have a seat at the local/county EOC?	Yes. If requested, an Operations Manager would be sent to the county EOC and would be assigned to the EOC Operations Section.

Insert additional rows as needed

Stakeholder Communications

Stakeholder	Primary Communicator	Frequency of Communications	Communication Modality
Staff	Court Administrator	At least weekly	Email or Mass Notification System
Judges	Presiding or Chief Judge	At least weekly	Email or Mass Notification System
Justice Partner/Building Tenants	Operations Director	Daily	Email, Phone, or Face to Face
Jurors	Jury Services Manager	Updates posted daily on court website	Public Website, Phone
Litigants/Witnesses/Parties	Local clerks/supervisors	As needed per hearing	Email and Phone
Media	PIO	As needed	Press Releases, Email, Phone
Employee Unions	HR Director	Daily	Email, Phone, or Face to Face
Public	PIO	At least weekly	Public Website, Social Media
Local/County EOC	COOP Coordinator	Daily	Email, Phone, WebEOC account with County
Sheriff's Office	Court Administrator	Daily	Email, Phone, or Face to Face
Local Bar Associations/Legal Service Associations	PIO (with assistance from Supervising Judges)	As needed	Email
State AOC	Court Administrator	At least weekly	Email and Phone
<i>Insert others</i>			

Last Resort Plan

In the event all primary forms of communication are not operable, how will communication and coordination occur?	If telecom is down, the plan will be to have the CMT meet in the parking lot of the downtown courthouse at 8am on the morning following the initial incident.
--	---

[Link to Template](#) (Fill out Table 2-11B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-12: EXPLORE HR CONSIDERATIONS

Contact Lists – As mentioned in the discussion regarding communications above (Step 2-11), keeping in contact with judges/staff is a priority in an emergency. Maintaining a contact roster of judges/staff, preferably electronic, is ideal. Investment in a mass notification system to send alerts (text and personal email) can greatly assist in quickly and efficiently contacting the court’s workforce. Having these contact lists available either in hard copy form, USB, or on a secure cloud website as a backup can prove helpful in an emergency. Contact rosters should include a mobile phone number, personal email, home address, and emergency contact at a minimum. The following Table 2-12A provides an example of guidance that may be useful for a court in regard to contact lists.

Table 2-12A: Workforce Contact Lists	
Item to Consider	Guidance Available
Who is responsible for collecting contact information?	All supervisors maintain an excel sheet that has personal contact info for all staff. The excel sheet is saved by the supervisor and is shared with their respective Department Director. Department Directors share the compiled excel sheets with the Court Administrator.
Where are rosters with all staff/judge contact information maintained?	Contact excel sheets are saved on a secure court server. Backup copies are saved on secure USB drives maintained by the Presiding or Chief Judge, the Assistant to the Presiding or Chief Judge and the Court Administrator. In addition, the court maintains a mass notification system where judges/staff self-report their personal contact information (personal email and mobile phone).
How often is contact information Audited?	Annually
Procedure for handling staff/judge injuries, death, notification of next of kin or other designated contacts.	In the event of an injury/death, the HR Director will reach out to the employee’s Department Director to obtain emergency contact information. HR will make all next of kin notifications if needed and report injuries/deaths to the local OSHA office.
<i>Insert others</i>	

[Link to Template](#) (Fill out Table 2-12A in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Another key aspect of HR communications pertains to how major injuries, deaths, and other important notifications to next of kin or other designated contacts will occur and who will be responsible for those notifications. In addition, certain employee injuries and deaths must be reported to the local OSHA office.

Employee Welfare – During an emergency, it is important to remember that judges/staff are often the survivors of the disasters themselves. Although court staff are designated as essential workers, the desire to continue the administration of justice must always be balanced with employee morale and welfare. Procedures should be developed to ensure management is checking in on staff well-being (e.g., individual supervisor-employee meeting and/or larger town hall style meetings). Many, if not most courts, offer services such as Employee Assistance Programs (EAP). While developing COOP plans, courts should explore what existing employee health benefits are offered and any additional services or programs they may be able to offer during a crisis. Disaster fatigue can settle in when an emergency continues not just for a few days or weeks, but for many months. Thus, exploring opportunities to promote the welfare and well-being of judges/staff, as well as methods to periodically check in on staff, should be addressed in the plan.

Staffing – In a major disaster, a court may face challenges due to staff/judicial absenteeism. Courts will need to determine how they will maintain essential functions with limited available staff, including possibly hiring temporary staff and/or rehiring retirees.

The following Table 2-12B provides an example of guidance that may be useful for a court in regard to employee welfare and staffing.

Table 2-12B: Employee Welfare and Staffing Strategies

Item to Consider	Guidance Available
Employee Welfare	
What services are available to help employee welfare during a crisis?	Court uses County Employee Assistance Program (EAP), Court has also partnered with Red Cross to bring in disaster mental health counselors onsite if needed (HR Director has contact information for Red Cross contacts). In a disaster, HR Benefits team will contact the three major employee health providers to assess what services they can provide to judges/staff either on or offsite.
How will disaster fatigue be addressed?	Periodic surveys will be sent to staff (at least monthly) to assess the court's response and the staff's pressing concerns. Townhall meetings will also be utilized to address if an emergency continues beyond 30 days.
<i>Insert others</i>	
Staffing Strategies During Emergencies	
Procedure for hiring additional staff on an interim basis (e.g., temp agencies, retirees, etc.)	HR Staffing Manager has contract with temp agency (Select Pro) to provide emergency hiring of temporary workers. HR Staffing also maintains a roster of all retirees to include their contact information and job titles when at the court.
Procedure for on how to obtain additional judges if there is a shortage of judicial officers available.	Operations Judicial Assistance Group maintains a list of temporary judges and retired judges that can be used in an emergency.
<i>Insert others</i>	

[Link to Template](#) (Fill out Table 2-12B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

HR Policies – Having emergency policies in place prior to a disaster can greatly help the court mitigate the variety of HR concerns that arise during a disaster. Emergency leave policies, approved prior to a disaster, can assist the court in potentially obtaining FEMA Public Assistance grant monies after a disaster. The following policies should be addressed in either a master HR emergency policy or separate policies:

- **Work schedules and compensation** – Do current policies address whether nonessential staff is paid during COOP plan implementation? What will be the guidance given to nonessential staff? Are there criteria under which staff can obtain cash advances, if needed? Can the court require essential functions staff to work overtime or on a compressed schedule to ensure the court is operational within a 12-hour period? Do COOP staff receive overtime payment if the normal workday is extended? Is there a policy for administering payroll if normal processes and databases are unavailable?
- **Flexible work hours and teleworking** – Do policies provide guidance for granting staff flexible work schedules and/or permission to work from home?
- **Obtaining additional staff support** – If additional staff is needed, are there streamlined procedures/guidelines for hiring temporary staff and/or consultants during an emergency?
- **Logistical support** – What accommodations (e.g., day care) are available for essential staff members who have dependents and are required to work after normal business hours? What options are available for staff members who need transportation to the alternate facility or temporary housing near the facility? Are staff members reimbursed for these and related expenses?
- **Discipline** – What does the court do if an essential functions staff member refuses to report for work?
- **Staff education and training** – Does the court have a policy requiring education about the COOP plan, staff roles and responsibilities during a disaster, and helping staff members prepare their families for emergency conditions (e.g., stockpiling water and nonperishable food, keeping a list of emergency phone numbers)?

The following Table 2-12C provides an example of guidance that may be useful for a court in regard to emergency HR policies:

Table 2-12C: HR Policies and Guidance

Personnel Areas	Specific Personnel Issue	Guidance Available
Work schedules and compensation	Payment of nonessential staff	HR Emergency Policy #XX-XX provides that the court will continue to pay non-essential staff as budget permits. Furlough and layoff process is included within this policy.
	Role of nonessential staff	HR Emergency Policy #XX-XX states that non-essential staff will remain home during the crisis. If telework is conducive to their position, it will be implemented. Nonessential staff can also be retrained or redeployed as needed.
	Overtime for essential functions staff	HR Overtime Policy #XX-XX governs how overtime can be used in a disaster. OT does not need to be approved by the Court Administrator but rather Department Directors
	Payroll administration when normal processes unavailable	HR Emergency Policy #XX-XX states that when payroll is not available, all staff will be paid the same amount they were paid from a prior pay period. Adjustments will be made within 60 days to correct for any errors.
	<i>Include additional issues here</i>	
Flexible work hours	Modification of work hours	HR Emergency Policy #XX-XX allows for modification of normal work hours for employees. This option may not be available for all job classifications and must be approved by a supervisor.
	<i>Include additional rows as needed</i>	
Leave	Emergency leave	HR Emergency Policy #XX-XX explains the various leave options that can be used in an emergency. The Presiding or Chief Judge has the discretion to allow for 80 hours of paid leave for staff in an emergency.
	<i>Include additional rows as needed</i>	
Obtaining additional staff	Emergency staffing	HR Emergency Policy #XX-XX addresses how standard hiring practices can be suspended (e.g., competitive examinations) and the use of temporary workers and bringing back retirees.
	<i>Include additional rows as needed</i>	
Logistical support	Emergency housing	HR Emergency Policy addresses how the Court Administrator can authorize the reimbursement of lodging and meals for those employees who need to be housed at an offsite location.
	<i>Include additional rows as needed</i>	
Discipline	Employee Discipline	The court's standard Policy and Procedures Manual (2012) discusses employee discipline. All policies contained in this document would apply during a disaster.
	<i>Include additional rows as needed</i>	
Education and training	Preparedness Training	No specific policy but court runs a CERT program to help train staff on how to prepare for disasters. Classes are held annually.
	<i>Include additional rows as needed</i>	
Telework	Telecommuting	Telework Policy #XX-XX directs how telework will be expanded in a disaster.
	<i>Include additional rows as needed</i>	
Other		
	<i>Include additional rows as needed</i>	

[Link to Template](#) (Fill out Table 2-12C in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-13: IDENTIFY THE RESOURCE MANAGEMENT PROCESS

Disasters will often require courts to procure items and resources quickly. Normal government procurement protocols may not prove timely, and thus there needs to be a strategy to procure resources in an expedited manner. A disaster procurement strategy should incorporate how emergency purchases are made.

Resource management also entails working with existing service providers and vendors. Some of the most important vendors to coordinate with prior to a disaster are the court's utility providers (e.g., power, water, gas). It is important to understand the redundancies in these systems and the court's priority for restoration. Asking these vendors if the court is considered an essential provider for critical restoration is helpful to ensure the courthouse can remain operational. If the courthouse has generators, identifying how those generators will be refueled is critical to ensure the continuity of power.

Courts should consider purchasing emergency supplies to prepare for a disaster. These could include basic emergency kits, USB charging devices, or laptop power banks. The court should also identify if there are any specific emergency supplies that may be needed for unique hazards (e.g., PPP equipment for pandemic situations or air purifiers and dust masks for courthouses near wildfire prone regions).

[FEMA's Ready Business Resource Management](#) website also provides some additional suggestions on resource management during disasters.

The following Table 2-13 provides an example of a completed resource management strategy.

Table 2-13: Resource Management Strategy

Item to Consider	Explanation, Response, or Protocol
How will emergency purchases be made? Who will take the lead in procuring and managing supplies in an emergency?	When COOP is activated, the Presiding or Chief Judge and/or Court Administrator can bypass normal procurement protocols and enact the emergency procurement strategy as dictated in the court's Procurement Manual. The court also has a verified government account through Amazon which allows for priority purchasing of goods for first responders. The court's Procurement Manager will serve as lead in obtaining and managing supplies for the court.
Which positions have access to court credit cards that can be used in an emergency? What is their limit?	Presiding or Chief Judge, Court Administrator, Procurement Manager, Finance Director, Facilities Director. Credit card limit on all cards are \$50,000.
What is the protocol for requesting resources from the local/county emergency operations center? What resources are they able to provide in an emergency?	Resource requests to the County EOC must be made through the court's Procurement Manager. Requests can be made either through the WebEOC portal or a County EOC request form #XX -XX and emailed to XXXX@countyec.org. County EOC can provide personal protective supplies, portable generators, emergency food/water, popup tents, trailers, and other emergency supplies as they have available. County EOC can also help promote any public messaging the court would like sent to the public.
What is the protocol for requesting resources from the State AOC? What resources are they able to provide in an emergency?	Resource requests to the AOC will be made through the Court Administrator. Court Administrator will submit an email/phone request to the AOC Facilities Director for what supplies are needed or call the 24/7 AOC Facilities number if AOC Facilities Director is unavailable. AOC can provide air purifiers, portable generators, building engineers, expertise on insurance related to the facilities, realtors to provide research on securing alternate sites, IT cybersecurity experts, and personal protective equipment.
Where is the list of critical vendors and contact information maintained? Who maintains it?	The procurement manager maintains a list of all critical vendors. List is backed up onto a USB drive and stored in the Facilities Director office and Procurement Manager office.
Have all courthouses been designated with priority utility service and for priority restoration after a disaster? Where are the emergency contacts for each utility stored?	Yes. All courthouses are exempt from rolling outages and have been designated to receive priority service. Meter numbers and utility contacts are stored in the local Facility Manager office.
What is the protocol to ensure courthouse generators (if applicable) are maintained and refueled during an emergency?	Generators undergo monthly preventative maintenance and yearly full load testing.
How long does each courthouse generator run, and what will it power?	All courts are equipped with fuel tanks to ensure generators will run at least 24 hours before refueling is required. Generators provide sufficient power to run the server room and all emergency systems in the courthouse.
What mutual aid agreements are in place with other court systems to provide aid in an emergency? What resources can be provided or shared?	Mutual aid agreements are in place with both the XXXXX County and XXXXX County court systems. The mutual aid agreement is stored in the Facilities Office. Resources to be shared include computers, servers, personal protective equipment, facility space, and personnel.
Where are court emergency supplies stored and maintained? (e.g., food, water, first aid, flashlights, dust masks, USB chargers, laptop power banks, etc.)? Include any hazard specific emergency supplies.	Emergency buckets are stored throughout each court facility (typically in break rooms). These buckets contain emergency food, water, flashlights, first aid kits, dust masks). Local facility managers know the exact locations of all buckets. Buckets provide enough emergency food/water to support all judges/staff for three days if needed. As wildfire smoke is a concern, all courthouses keep a supply of 100 dust masks in the event of a poor air quality event.
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Link to Template](#) (Fill out Table 2-13 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-14: DEVELOP A DEVOLUTION PLAN

The court’s devolution plan describes what to do if a catastrophic event renders leadership and essential staff incapacitated and/or renders the courthouse and alternate facilities nonfunctional. During devolution, the court would transfer authority and responsibility for essential functions to officials in another court. Devolution is something that should be coordinated with the State AOC as court jurisdiction could be limited to specific county or geographical boundaries. Efforts to move court operations out of normal jurisdictional boundaries should be coordinated with the State AOC as emergency orders may need to be generated to accommodate the legal transfer of jurisdiction. In some cases, a court may not realistically be able to devolve because of legal implications and/or restrictions. In other cases, a court may determine that some restrictions can be suspended during emergency conditions. A sample devolution plan can be found in Table 2-14 below:

Table 2-14: Devolution Plan		
Provide contact information for alternate court(s) available to perform essential functions (Add as many rows as necessary)		
Court	Contact Information	Is there a written agreement with the alternate court(s)?
XXXXX County	John Doe, Court Administrator, johndoe@court.gov , (XXX) XXX-XXXX	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
XXXXX County	Jane Doe, Court Administrator, janedoe@court.gov , (XXX) XXX-XXXX	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
List the officials and their successors (by position) allowed to transfer authority to perform essential functions (Add as many rows as necessary)		
Succession	Title	
Primary Official	Presiding or Chief Judge	
Successor	Court Administrator	
Successor	Operations Director	
Provide a plan for transferring essential records and other materials necessary for performing essential functions to alternate court(s). For example, will essential records and materials be stored and updated on the same schedule as those stored with alternate facilities?		
Court IT Director will meet with their counterpart at either XXXXX County Courts or XXXXX County Courts to provide login credentials for their staff to access all cloud-based case management systems needed to move essential functions over to their County. Because HR and Purchasing programs are run through the State AOC, IT Director will inform State AOC that login credentials need to be accessed by XXXXX/XXXXX County Court systems. Non-cloud-based applications (e.g., Protective Order Database) will need to be configured so the alternate court can access or potentially move server to alternate court location.		
List procedures for notifying the alternate court of devolution.		
The Presiding or Chief Judge will have a conference call with both the State Chief Justice and the Presiding or Chief Judge of the alternate court of devolution. This conference call will determine if devolution is necessary and if the alternate court can absorb the court’s essential functions. It will also set the parameters of what specifically will be devolved over to the alternate court. Once this call occurs, the Presiding or Chief Judge will debrief with the CMT on the next steps.		
List procedures for returning authority once the court is reconstituted.		
If devolution is underway, there will be a weekly conference call between the Presiding or Chief Judge and the alternate Presiding or Chief Judge to assess the status of devolution operations. Once the time comes to end the devolution process, the Presiding or Chief Judge will have a conference call with both the State Chief Justice and the Chief Judge of the alternate court of devolution. This conference call will determine when to return authority from the alternate court.		
Are there any essential functions that are unable to be transferred to another court system due to law, regulation, or statute?		
Juvenile Court is not allowed to be taken outside of our county jurisdiction per state regulations.		

[Link to Template](#) (Fill out Table 2-14 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PART B: ACTIVATING COOP IN A DISASTER OR EMERGENCY

STEP 2-15: IDENTIFY COOP ACTIVATION TRIGGER POINTS AND ACTIVITIES

It is important to identify the conditions under which the COOP plan will become activated and who has the authority to activate the plan. COOP activation can sometimes be obvious (e.g., major earthquake strikes a locality, global pandemic, etc.). However, there may be other incidents that are very court specific that can have a significant impact on a court, but the surrounding locality is not impacted (e.g., targeted cyberattack, extended loss of utilities at a single courthouse, asbestos release in a courthouse). The COOP response should be flexible and scalable based on the specific emergency incident, and not every crisis is going to require the court to implement all aspects of the COOP plan. For example, in a cyberattack scenario, alternate facilities may not be needed. Other emergency events may not require any activation of the COOP. For example, a fire emergency may require a short-term evacuation of the court facility followed by the resumption of normal operations without the activation of the COOP.

Incidents can occur both during and after work hours. Thus, identifying trigger points during these timeframes can also assist in knowing when to activate a COOP.

The following Table 2-15A provides a list of considerations for when to activate the COOP plan and a list of questions to help assess activation trigger points.

Table 2-15A: COOP Activation Considerations
General Considerations For When to Activate the COOP
<input type="checkbox"/> Direction and guidance from higher authorities (e.g., Mayor, Governor, President, Public Health Officials).
<input type="checkbox"/> The health and safety of staff.
<input type="checkbox"/> The ability to execute court essential functions.
<input type="checkbox"/> Changes in threat or weather advisories.
<input type="checkbox"/> The functioning of critical infrastructure (including communications systems, information systems, facilities, and other vital equipment).
<input type="checkbox"/> The potential impact on critical court justice partners (e.g., court security staffing, clerk of the court, prosecutor's office, public defender's office, etc.).
<input type="checkbox"/> The expected duration of the emergency.
<input type="checkbox"/> <i>Insert others</i>
Questions to Assess COOP Activation Trigger Points
<input type="checkbox"/> Is the threat aimed at the courthouse, personnel, or surrounding area?
<input type="checkbox"/> Are employees unsafe remaining in the courthouse and/or area?
<input type="checkbox"/> Is it safe for employees to return to work the next business day?*
<input type="checkbox"/> What is the status of the courthouse building infrastructure? (e.g., building structure, water, electricity, gas, HVAC and IT systems)
<input type="checkbox"/> Will building infrastructure systems be operational the following business day? (e.g., building structure, water, electricity, gas, HVAC and IT systems)*
<input type="checkbox"/> Can pressing matters be sent to another courthouse with minimal impact to normal operations?
<input type="checkbox"/> Are courthouse occupants affected? Have they evacuated or sheltered in place?*
<input type="checkbox"/> What are the instructions from first responders?*
<input type="checkbox"/> What pressing matters or cases with time constraints remain on the court calendar for the remainder of the day?*
<input type="checkbox"/> <i>Insert others</i>
Note: * indicates events occurring after work hours; ** indicates events occurring without warning

[Link to Template](#) (Copy and paste the text from Table 2-15A above into the corresponding Table 2-15A in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Table 2-15B is a generic activation checklist to utilize when activating the COOP.

Table 2-15B: COOP Activation Checklist
Initial Status Briefing, Assessment and COOP Activation
<ul style="list-style-type: none"> <input type="checkbox"/> COOP Coordinator sets up conference call or In-person meeting with CMT for current situation status briefing (sample briefing format found in Communications Section). <input type="checkbox"/> Presiding or Chief Judge and/or Court Administrator decides to activate COOP. <input type="checkbox"/> COOP Coordinator sends alert notification to all managers regarding COOP activation. <input type="checkbox"/> Facilities staff conducts assessment of the building(s) (if threat/hazard may have impacted facilities) and begin coordinating repairs with appropriate vendors. <input type="checkbox"/> <i>Insert others</i>
Crisis Management Team (CMT) Activation
<ul style="list-style-type: none"> <input type="checkbox"/> Retrieve the current COOP (virtual or hard copy) and review this Activation Checklist. <input type="checkbox"/> Provide court wide communication to all staff and judicial officers as to the current situation status. <input type="checkbox"/> Assess what communication needs to be sent to critical justice partners (e.g., prosecutor's office, public defender's office, etc.) <input type="checkbox"/> Assess if courthouse(s) should remain open or closed. <input type="checkbox"/> Assess how the court's essential functions are impacted. <input type="checkbox"/> Assess if alternate facilities need to be implemented and if judges/staff need to deploy to fulfill essential functions offsite or remotely. <input type="checkbox"/> Assess how to handle judges/staff not performing essential functions. Should they report home? Telework? Remain onsite? <input type="checkbox"/> Assess how to handle trials currently in progress. <input type="checkbox"/> Assess how to handle jurors and what communication needs to be sent to onsite and summoned jurors. <input type="checkbox"/> Assess if an emergency order is needed from the court of last resort. <input type="checkbox"/> Assess if any emergency HR policies need to be enacted. <input type="checkbox"/> Assess courthouse security to include information on inmate movement, availability of security staffing, securing entrances, any other safety measures to protect judges/staff. <input type="checkbox"/> <i>Insert others</i>
Department Managers Activation
<ul style="list-style-type: none"> <input type="checkbox"/> Assess the welfare of staff and determine availability of staff to remain working. Report injured or missing employees through their chain of command and to HR. <input type="checkbox"/> For after-hours events, assess which critical staff needs to be notified before the following business day and make contact as appropriate. <input type="checkbox"/> Assess unit's facility space for any damage or concerns. Report information to Facilities Management. <input type="checkbox"/> Review essential functions. Prioritize essential functions based on existing workload and determine if Return Time Objectives (RTO's) can be accomplished. <input type="checkbox"/> Identify critical staffing/resource requirements and health/safety concerns. <input type="checkbox"/> Identify communication concerns and assess the unit's IT equipment and applications. Determine which essential records, software, applications, etc. are needed. <input type="checkbox"/> Discuss any internal or external messaging that needs to be completed. <input type="checkbox"/> Based on available staffing, existing resources, and work area condition, begin to assess if essential functions can continue in current facility. Report the operational status and any relevant action steps through the chain of command. <input type="checkbox"/> Assess and secure the unit's Go Kit in case of relocation. <input type="checkbox"/> Notify any support agencies or critical contacts of the COOP activation <input type="checkbox"/> <i>Insert others</i>
Other Key Stakeholder Activation
<i>Insert important action steps that need to occur</i>

[Link to Template](#) (Copy and paste the text from Table 2-15B above into the corresponding Table 2-15B in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PART C: ONGOING COOP OPERATIONS DURING A DISASTER OR EMERGENCY

STEP 2-16: IDENTIFY KEY ROLES/RESPONSIBILITIES DURING A CONTINUITY EVENT

The following Table 2-16 provides a high-level overview of the general responsibilities that various court departments have during a COOP event. Many of these could be considered essential functions or could be supporting activities to essential functions. The table is presented in the form of a checklist to ensure the key roles/responsibilities of court departments are not overlooked in a continuity event. COOP planners should customize this checklist based on their individual court's specific operations and responsibilities.

Table 2-16: Key Roles/Responsibilities During a Continuity Event	
COOP Coordinator/Emergency Management	
<input type="checkbox"/> Provide guidance to the CMT on existing court emergency plans and procedures. <input type="checkbox"/> Assist with crisis communications in collaboration with the Court Public Information Officer. <input type="checkbox"/> Coordinate and facilitate situation status conference calls/in-person meetings as needed for the CMT. <input type="checkbox"/> Serve as primary liaison to the local/county Emergency Operations Center (EOC). Provide resource requests to the County EOC as needed. <input type="checkbox"/> <i>Insert others</i>	
Court Operations	
<input type="checkbox"/> Assess and determine courtroom operation capabilities based on available staff. <input type="checkbox"/> Triage calendars to determine which critical hearings must proceed and which could be continued. <input type="checkbox"/> Coordinate with facility managers to set up triage tables outside the courthouse to assist public on how their case is being handled and where to make payments or filings. <input type="checkbox"/> Coordinate with court security managers on security needs. <input type="checkbox"/> Coordinate with security transport managers on the scheduling of in-custody transportation and bailiff requests. <input type="checkbox"/> Ensure critical case files and or paperwork is preserved. <input type="checkbox"/> Coordinate the transfer of cases to court or non-court facilities as stated in the Alternate Facilities portion of the plan. <input type="checkbox"/> Provide communication to parties affected by the incident and coordinate information to justice partners. <input type="checkbox"/> Provide timely information and direction to existing and prospective jurors. <input type="checkbox"/> <i>Insert others</i>	
Finance	
<input type="checkbox"/> Monitor cash flow and provide guidance to the CMT on the financial status of the court. <input type="checkbox"/> Set up and communicate jobs codes in order to track emergency spending for possible FEMA reimbursement. <input type="checkbox"/> Assist with any emergency procurements or contracts needed to respond to the incident. <input type="checkbox"/> Ensure continuity of payroll for staff and judges. <input type="checkbox"/> <i>Insert others</i>	
IT	
<input type="checkbox"/> Assess and restore IT infrastructure (e.g., computer rooms, network, internet, phones). <input type="checkbox"/> Assess and restore critical applications needed to fulfill the court's essential functions. <input type="checkbox"/> Provide IT technical support for judges/staff who are displaced to another work location. <input type="checkbox"/> Repair or replace IT equipment to support essential functions. <input type="checkbox"/> As telework may be a critical tool in order to complete mission essential functions, IT should be prepared to increase the amount of approved staff who need access to effectively telework. <input type="checkbox"/> There may be increased use of videoconferencing due to a lack of a facilities. As such IT should be ready to mobilize videoconference systems at all courthouses and/or move existing systems to an alternate facility. IT should also ensure network bandwidth is monitored to maintain operations with increased demand on videoconferencing or telework. <input type="checkbox"/> <i>Insert others</i>	
Human Resources	
<input type="checkbox"/> Monitor and process paperwork related to staff/judge injuries and deaths.	

<input type="checkbox"/> Provide guidance on modification of staff work schedules, job duties, or work location. Address any grievance issues that may arise. <input type="checkbox"/> Provide ongoing communication to respective bargaining units regarding staff deployment, working conditions, and job functions during the incident. <input type="checkbox"/> Work with external behavioral health resources to provide crisis counseling for staff affected by the incident. <input type="checkbox"/> Assist in staff accountability by responding to manager requests for employee contact information. <input type="checkbox"/> Provide direction on related leave and other HR policies/protocols. <input type="checkbox"/> Provide guidance on any emergency benefits (e.g., health, dental, childcare, COBRA, etc.) <input type="checkbox"/> <i>Insert others</i>
General/Legal Counsel
<input type="checkbox"/> Complete Judicial Emergency Orders as needed. <input type="checkbox"/> Provide guidance to judges on how cases can be appropriately handled during emergency incidents. This will include interpretation of how Judicial Emergency Orders apply to their specific case types. <input type="checkbox"/> <i>Insert others</i>
Facilities
<input type="checkbox"/> Assess facility damage and coordinate with applicable vendors to provide repair. <input type="checkbox"/> Coordinate any environmental testing to ensure safe workspaces. <input type="checkbox"/> Provide office supplies to units performing essential functions. <input type="checkbox"/> Facilitate moves using internal resources or external moving companies to transport staff/resources to needed areas. <input type="checkbox"/> <i>Insert others</i>
Public Information Officer
<input type="checkbox"/> Develop and distribute press releases through all available media outlets. Of concern will be which facilities and services are still available to the public during the COOP activation. <input type="checkbox"/> Ensure the court's social media platforms and public website are updated with current information <input type="checkbox"/> and inquiries on social media platforms are being addressed. <input type="checkbox"/> Coordinate any press conferences as appropriate. <input type="checkbox"/> Liaison with other Public Information Officers (e.g., city, justice partner, law enforcement) to ensure accurate and unified messaging to the public. <input type="checkbox"/> <i>Insert others</i>
Insert other departments as necessary
<i>Include key action steps this department would take during a continuity event</i>

[Link to Template](#) (Copy and paste the text from Table 2-16 above into the corresponding Table 2-16 in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PART D: RECONSTITUTION AND COST RECOVERY

STEP 2-17: IDENTIFY THE RECONSTITUTION PROCESS

Reconstitution includes procedures to terminate alternate operations and resume normal operations. The court should identify and outline a plan to return to normal operations once the CMT determines the disaster or emergency no longer poses a threat. In addition to facilities-related challenges, there will likely be challenges related to workload, depending on the nature of the disaster. For example, following a major storm with catastrophic damages, there may be an influx of certain case types including family, probate, property, and insurance cases. The public may need help in showing title to property to qualify for expedited assistance from FEMA. Family law cases may see issues with relocating children outside a jurisdiction, establishing guardianships, determining custody, and issuing emergency protection orders.

Reconstitution is not a single event but rather a planning process that involves consideration of how to restore operations at the courthouse. Bringing a court's operations back online cannot be accomplished through one individual; therefore, the court should adopt a team approach to restore operations. A cross functional team made of the units below helps create a well-rounded Reconstitution Team:

- Facilities
- IT
- Courtroom Operations
- Human Resources
- Representative of legal owner of the courthouse (e.g., This could be the State AOC)

The following Table 2-17A provides a basic checklist of action items the Reconstitution Team will implement to help bring the court back into normal operations.

Table 2-17A: Reconstitution Team Responsibilities

- Conduct an initial assessment on the status of court facilities.
- Implement procedures to direct court officials to assess the condition of the court facility to determine the extent of damage and options for repairing, rebuilding, replacing, or moving court facilities. In addition, court officials should determine if there are personnel issues to address (e.g., some staff no longer work for the court as a result of the disaster) and the condition of court records to determine whether restoration services are needed.
- Communication between senior leadership and building managers or repair crews.
- Recovery of resources from the damaged building (if safe to do so).
- Coordination of repairs and procurement of resources to re-occupy the damaged facility.
- Procurement of new permanent or semi-permanent facility.
- Creation of a return-to-work schedule to recover operations in the order of greatest need (often the essential functions will continue from the alternate location until the new permanent one has been tested and proved fully operational).
- Creation of a schedule to phase down operations at the alternate facility and return activities, staff, records, and equipment to the court's old, temporary, or new facility. The schedule should allow information and resources from the alternate facility to be transferred to the primary facility with minimum disruption to the performance of essential functions.
- Development of communication plan to relay information to staff. Once the plan has been developed, the information coordinator or other designated court official should inform all essential and nonessential staff, that the emergency is over, that a process has been developed to resume normal operations, what the general process entails, and that staff members will be informed of their specific duties as the plan is implemented. All parties also should be notified once essential functions at the alternate facility have been transferred successfully to the court's primary facility and the COOP plan implementation has been terminated
- Insert others*

[Link to Template](#) (Copy and paste the text from Table 2-17A above into the corresponding Table 2-17A in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

The following Table 2-17B outlines how reconstitution logistics can be managed at the court.

Table 2-17B: Reconstitution Logistics	
Item to Consider	Explanation, Response, or Protocol
Who will comprise the Court's Reconstitution Team?	Facilities Director, HR Director, Court Operations Manager, IT Director, AOC Facilities Analyst
Who will oversee leading the Reconstitution Team?	Facilities Director
What facilities assessments are done for reconstitution?	Facilities Managers at local courthouses keep a damage assessment form and checklist. This checklist will be utilized to assess how much damage the courthouse has received and will report back to the Facilities Director. Facilities Director will provide a report to the CMT. Depending on the nature of the hazard, a different analysis may need to be completed. For example, if the threat is a cyberattack, the IT unit will be responsible for conducting a cyber assessment.
Who is responsible for developing communication to the various court stakeholders during the reconstitution process?	The Court Operations Manager will be responsible for sending out weekly communication to the various stakeholders in the reconstitution process. This will include our building tenants since many of them reside in our court.
What is the role of the State AOC during reconstitution?	All courthouses are owned and insured by the State AOC. The AOC will be a part of the reconstitution team and will ultimately be responsible for managing the construction contracts and overall project management to rehabilitate the courthouse. Ultimately, the AOC is responsible for repairs to the building and paying for these repairs. AOC will determine through their insurance company if a total demolition/renovation is needed or if repairs will suffice.
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Link to Template](#) (Fill out Table 2-17B in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-18: IDENTIFY THE COST RECOVERY PROCESS

Court COOP plans have not traditionally included a cost recovery section. However, the lessons learned from recent disasters have indicated that, at least for some courts, it is an important topic and should be addressed in either a supplemental annex or embedded within the court's COOP. The decision to include a cost recovery section may depend on first identifying what entity is responsible for cost recovery (e.g., the local court, State AOC, county executive branch, or state executive branch).

Cost recovery generally pertains to grant programs run through the federal government and state governments to assist government entities to make repairs to buildings and pay for some expenses incurred as a result of the disaster. For courts that may have a part in cost recovery processes following a disaster, it is critical to understand what programs are available, how the application processes work, and how to manage awarded grant funds. Typically for court organizations, the roles and responsibilities vary significantly by state depending on variables such as court organizational structure and facility ownership/responsibility. To determine if cost recovery should be included in the court's COOP plan, the COOP Planner should meet with the State AOC as well as state and/or local emergency management entities to understand cost recovery processes, roles and responsibilities for his or her court.

The largest cost recovery program in the nation is the [Public Assistance \(PA\)](#) grant program, administered by FEMA, which provides federal assistance to government organizations and certain private nonprofit organizations following a Presidential disaster declaration. Through the PA grant program, FEMA provides supplemental assistance for debris removal, life-saving emergency protective measures, and the repair, replacement, or restoration of publicly owned facilities that have been damaged in a natural disaster. The PA program also seeks to protect facilities from future damage by funding hazard mitigation measures during the recovery process. It is important to note that FEMA follows federal procurement standards, and often courts will

need to follow the FEMA guidelines if they are to seek reimbursement. More information about the FEMA PA and rules surrounding emergency procurement can be found on the FEMA website.

Cost Recovery, like Reconstitution, is a team project. Although there may be one person who will take the lead, often it takes a team to complete the extensive work often required to complete a PA application to obtain reimbursement. Suggestions of who should be on the court’s Cost Recovery Team include:

- Grants Manager
- Accounting
- Procurement
- Facilities

It is helpful to identify a person who will take the lead in cost recovery grant applications. This person will often require training to understand the application process, procurement rules, and state/local emergency management coordination issues. To help keep track of eligible costs, it is recommended courts set up a job code in advance to track not only supplies but personnel costs associated with a disaster.

The following Table 2-18 identifies who will be part of the Cost Recovery Team and provides direction on how the process will be implemented following a disaster.

Table 2-18: Cost Recovery Logistics	
Item to Consider	Explanation, Response, or Protocol
Who will comprise the court’s Cost Recovery Team?	Finance Analyst, Accounting Manager, Procurement Manager, Facilities Manager
Who will oversee and lead the Cost Recovery Team?	Finance Analyst
What job code (or other mechanism) will be used to track services, supplies, and personnel costs associated with the emergency?	Code #XXXX will be used to track personnel costs in the court’s online timekeeping system. Code #XXXX will be used to track any services and supplies made during a COOP incident. The finance analyst will be responsible for sending court wide email informing everyone that the above job codes are to be used, parameters of their use, and when to discontinue use of the job codes.
Which entity is responsible for applying for FEMA Public Assistance (Court, AOC, County Emergency Management, etc.)?	Ultimately, our local court will be responsible for putting together the FEMA PA application. If there are damages to the facility, the State AOC will assist our court in the application, but the application process will be run out of our local court. County emergency management has requested that they be informed when we make a PA application.
What is the overall process by which the Court will track and submit costs during an emergency and ensure FEMA procurement rules are followed?	Cost Recovery Team will meet on a bimonthly basis during a crisis to assess costs related to the disaster and what may be eligible for PA reimbursement. An excel sheet will be created and maintained by the accounting unit that will track all expenses and what expenses will be submitted to FEMA/state for reimbursement. The procurement manager will oversee how services/supplies are purchased to ensure we are following FEMA procurement rules. Reminders will be sent to Facilities staff and others who purchase items on behalf of the court with reminders on the rules of FEMA procurement standards.
How are the courthouses currently insured? Where are the insurance documents located?	The court is currently insured by the State AOC. AOC Facilities Analyst assigned to the court maintains the insurance documents. As a backup, the Facilities Director and Procurement Manager maintain copies of those insurance documents on USB devices.
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Link to Template](#) (Fill out Table 2-18 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

STEP 2-19: DEVELOP AN AFTER-ACTION REVIEW PROCESS

No matter how prepared a court is for an emergency, there will always be lessons learned once a disaster strikes. Elements in the COOP plan which were initially thought to be sufficient may not work out either in an exercise or a real incident. Hence, it is important to document significant actions, decisions, and steps taken during an emergency to develop an after-action report.

FEMA recommends using the [Homeland Security Exercise and Evaluation Program](#) (HSEEP) to conduct after-action reviews and reports. The HSEEP process is a very detailed approach to critically assess the court's response to a crisis. Even if the court does not utilize the full HSEEP process, simply having a meeting where the CMT discusses what went well, what didn't go well, and action steps to help address deficiencies can serve to help capture this critical information. It is helpful to look beyond just the CMT to ensure lessons learned are gathered from all key stakeholders. This could include meetings or surveys with justice partners, line staff, and various judges to obtain a holistic picture of the response. To ensure the process is completed, the responsibility of developing an after-action report must be assigned to a specific individual. Whatever process a court uses, it is important to set aside time for this assessment once the crisis ends, and to document it in writing. Any lessons learned should also be incorporated into the COOP plan and other emergency plans.

The following Table 2-19 is an example of how after-action reporting can occur:

Table 2-19: After-Action Review	
Item to Consider	Explanation, Response, or Protocol
Who will be responsible for leading the after-action review?	COOP Coordinator
What methodology will be used to develop an AAR? (e.g., surveys, meetings, one on one interviews)	In-person meeting with the CMT, all staff/judge surveys, 1:1 meetings as needed with key stakeholders involved in the response. County emergency management will be invited (if deemed appropriate) to help share lessons learned with our local emergency management partners.
How quickly will a written AAR be developed following the conclusion of an emergency incident?	No longer than 60 days following the conclusion of the emergency.
A written copy of the AAR will be distributed to the following stakeholders.	CMT
Each of the following areas will be evaluated during an AAR.	Communication – Internal/External Ability to continue essential functions Creative solutions Strengths Areas for improvement <i>Insert others</i>
A Correction Action Plan (CAP) will be developed to capture action items learned from the AAR. Who will be responsible for ensuring the items listed in the CAP are implemented?	COOP Coordinator
Where will completed after-action reports reside?	Internal document library on the court's emergency preparedness intranet site.
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Link to Template](#) (Fill out Table 2-19 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

SECTION III: FURTHER COOP CONSIDERATIONS

TRAINING AND EXERCISE PROGRAMS

Once a base COOP plan has been substantially completed as outlined in Section II, it is important for courts to consider additional steps to ensure the COOP plan remains a living and actionable document. Two primary activities that will foster this objective are the development of training and exercise programs, and the development of specific hazard annexes to supplement the COOP plan. These are detailed individually in the following steps and examples provided in Section III.

STEP 3-1: IDENTIFY A TRAINING AND EXERCISE PROGRAM

The information contained in the COOP plan will be of limited value if it is not accompanied and supported by a rigorous regimen of formal training, testing, and exercising. These activities should be identified, and programs should be set to a regular schedule.

Training is a valuable tool for helping principal stakeholders to understand their specific roles/responsibilities in the COOP plan. Conducting a series of orientation workshops/trainings to familiarize individuals with the plan is a good start. Developing a marketing campaign, strategy, or even a slogan can assist in getting the word out and building up the importance of the plan. Combining training sessions and exercises can be used as an adult learning strategy to more effectively teach COOP concepts (e.g., seminar, workshop, drill, tabletop, functional, or full-scale exercise).

Ideally, whoever serves as the COOP Coordinator or COOP Planner for the court will be the person to ensure training and exercises are taking place. This person will need the support of the Presiding or Chief Judge and Court Administrator to ensure all levels of the organization are involved in training and exercise activities.

It may be helpful to initially train the Crisis Management Team (CMT) members to ensure they are aware of the plan and their role within it. As a subsequent step, developing additional trainings for specific teams (e.g., Cost Recovery Team, Reconstitution Team) can be helpful so that the team members gain familiarity with each other and are aware of the specific preparation steps they can take prior to a disaster. Moving forward, the CMT and applicable stakeholders should be made aware of any updates as they are made to the COOP plan.

Quick Reference Guides - The sheer volume of information contained within many COOP plans can be overwhelming and it is important to identify the specific COOP topics that staff of different departments need to be trained on. The court may consider developing quick reference guides to assist court management in their COOP roles/responsibilities.

Tabletop Exercises - Conducting simulated tabletop exercises for your CMT is a no-cost method for teaching COOP plan protocols and procedures. It allows staff to internalize key COOP plan elements and serves as a tool for testing and assessing the COOP plan for ongoing refinement. In addition, exercises can facilitate the court's efforts to get plan buy-in from staff and other stakeholders.

Additional Resources for Training and Exercises - The court may want to explore reaching out to the local FEMA Regional Continuity Manager and/or local emergency management office for assistance in developing their training program. These entities can often provide training materials and technical resources, or can even help facilitate workshops and/or exercises. Typically, local emergency management offices conduct their own COOP exercises and may be open to inviting court participation in those exercises where feasible and beneficial. Exercises can require a significant amount of work to plan and conduct; therefore, reaching out to partners like

FEMA and the local emergency management office for assistance can be helpful. In addition, FEMA provides a variety of exercise support resources through its [National Exercise Division](#), offers a series of [Virtual Tabletop Exercises](#) through its Emergency Management Institute, and offers a [Sample Tabletop Exercise](#) on its website. FEMA training and exercise support resources are provided at no cost to the court.

The following Table 3-1 is an example of how to formalize a training and exercise program:

Table 3-1: COOP Training and Exercise Program Identification Worksheet			
Type of Training	Recipients	Method(s)	Frequency
COOP Orientation	All managers/judges	In-person training program	Upon initial hire
	New managers/judges	Online refresher	Annually
	Justice partner stakeholders	In-person training program	Annually
COOP Refresher	CMT	In-person training	Bi – Annually
	Reconstitution Team	In-person training	Annually
	Cost Recovery Team	In-person training	Annually
Updates to FEMA Cost Recovery Process	Cost Recovery Team	In-person training	When FEMA processes change
<i>Insert others</i>			
Exercises			
Type of Exercise	Recipients	Method(s)	Frequency
Drill	All judges/staff	Fire Drill	Annually
Tabletop	CMT	In-person tabletop	Annually
Functional	Emergency Management	Collaborate with local EOC	Annually
Full Scale	CMT	Alternate Facilities Exercise	Every two years
<i>Insert others</i>			

[Link to Template](#) (Fill out Table 3-1 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

DEVELOPING ANNEXES

STEP 3-2: CONDUCT A HAZARD ANALYSIS TO IDENTIFY NEEDED ANNEXES

As mentioned previously in this Guide, the COOP plan forms the foundation for determining how the court will respond to a disaster or emergency and continue its essential functions. A court’s Emergency Operations Plan/Occupant Emergency Plan is established to determine the policies and procedures dictating the response to short-term emergencies (e.g., fire alarm activation, bomb threat, medical emergency, or brief power outage). These two documents form the bedrock of its emergency management program. Looking beyond these two foundational plans, it is helpful for the court to evaluate if there are specific hazards that the court faces that present an elevated threat and that should be addressed through an Annex to the court’s COOP plan. The core elements in the COOP plan (e.g., essential functions, communication, CMT, etc.) should remain applicable regardless of the hazard, but some disasters may require additional planning efforts and response.

Some of the potential hazards that all courts across the nation face include acts of terrorism, cyberattack, ransomware, extended civil unrest, and extended power loss, to name a few. However, based on geographic location, a court may also face unique threats such as earthquakes, tornadoes, wildfires, flooding, and/or hurricanes. These hazards each present unique emergency planning and response considerations. For example, in an earthquake scenario, it is important to identify the person(s) who have the responsibility to determine a building is safe for entry after the shaking subsides. In a hurricane scenario, it is important to identify the person(s) who have the responsibility to determine which phase of the storm would be considered a trigger for closing the courts. For a cyberattack scenario, it is important to identify the person(s) who have the responsibility to determine what protocols are in place in the event the court’s public webpage gets hacked?

Conducting a hazard analysis, like the example shown below, can help the court prioritize the development of COOP plan annexes. To complete this basic analysis, a planner would input all the types of hazards that could impact the court (human or natural caused). Once listed, the hazards are assessed according to their probability and severity. They are then ranked according to their total risk. Hazards with the highest risks are the ones the court should consider developing annexes for. Table 3-2 below illustrates a sample hazard analysis.

Scoring Factor	Hazard					
	Cyberattack	Earthquake	Flooding	Pandemic	Power Loss	<i>Insert others</i>
Probability (1-5) One means low probability of occurrence and five meaning a high probability of occurrence.	4	2	3	5	4	
Severity (1-5) One means low impact to court functions and five meaning a critical impact to court operations.	4	5	2	4	2	
Total Risk (P x S) Multiply probability by severity to attain total risk score.	16	10	6	20	10	

[Link to Template](#) (Fill out Table 3-2 in the COOP template with the appropriate information for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Below are additional resources for courts considering implementation of a more detailed hazard analysis:

- [FEMA risk/hazard assessment guide](#)
- [California Hospital Foundation hazard vulnerability analysis](#)

STEP 3-3: DEVELOP COOP ANNEXES

COOP annexes, in effect, are supplemental COOP plans that address the unique planning and response considerations for a given hazard. Developing annexes should be the responsibility of the COOP Planner or emergency management lead. Similar to the process of developing the base COOP plan, the process may necessitate convening a representative planning team to provide input into the development of the annex as the roles and responsibilities assigned to the CMT, department heads, and court staff may vary considerably based on the hazard type. Planners would be wise to remember that COOP plans and annexes should never be written in a silo, but rather should be developed through a cross-functional, collaborative process.

Annexes will vary considerably based on the hazard type. The sample annex provided in the following pages is specific to the COVID-19 pandemic and includes possible language that a court could consider for use in its own pandemic annex where applicable. It should be noted that annexes for different non-pandemic events may contain different components as dictated by the hazard type.

SAMPLE PANDEMIC ANNEX FOR A NOVEL VIRUS

PANDEMIC ANNEX PART A: READINESS AND PREPAREDNESS

Table 3-3A: Purpose of Pandemic Annex

A pandemic is unlike other types of public health emergencies because it has the potential to rapidly cause illness in large numbers of people worldwide with continued transmission for months. It will not directly affect the physical infrastructure of the organization. The ease with which a virus strain transmits from person-to-person, the susceptibility of the population to it, and the severity of illness resulting from it are all factors that determine the court's level of response. Protecting the health and safety of court judges/staff must be the focus of planning in order to ensure the continuity of court essential functions.

This COOP annex contains guidance intended to assist the court in maintaining essential functions in the event of a pandemic. The guidance is specific to pandemic events and supplemental to the court's base COOP plan. The core elements included in the base plan (e.g., essential functions, communication, CMT, etc.) remain applicable.

[Link to Template](#) (Copy and paste the text from Table 3-3A above into the corresponding Table 3-3A in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Table 3-3B: Continuity Objectives for Pandemic Events

The overarching objectives in a pandemic include:

- Ensure the health and safety of judges/staff
- Ensure the continuous performance of essential functions and operations.
- Communicate pandemic preparedness, response and recovery guidance to judges/staff.
- Maintain an open and ongoing dialogue with justice partners (e.g. Prosecutor Office, Public Defender, Probation, Social Services, etc.) to ensure the continuity of critical justice system functions for the local community.
- Achieve a timely and orderly recovery from a pandemic event and resumption of full service to the public.

[Link to Template](#) (Copy and paste the text from Table 3-3B above into the corresponding Table 3-3B in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Table 3-3C: COOP Planning Assumptions for Pandemic Events

The following are typical assumptions the court may face in a pandemic incident caused by a novel virus.

- The epidemiological characteristics of a novel virus may differ from those of seasonal influenza or other viruses.
- Transmission is likely to be primarily by droplet spread; there may also be contact and possible airborne transmission. Therefore, especially early in the pandemic before the characteristics of the virus are well established, infection control recommendations may include standard, airborne and contact precautions, including eye protection.
- The epidemiologic profile (i.e. virulence, principal mode of transmission, timing and duration of viral shedding, and attack rate in different risk groups) of the pandemic may change during each pandemic phase and wave, and recommendations regarding specific measures may need to be adapted over the course of the pandemic.
- The effectiveness of non-pharmaceutical containment measures is unknown and depends on timing of implementation, compliance among the targeted populations and characteristics of the novel virus.
- Some community containment measures may need to be in place for as long as 12 weeks, possibly even longer.
- Rates of absenteeism will depend on the severity of the pandemic. In a severe pandemic, absenteeism attributable to illness, the need to care for ill family members and fear of infection may reach 40% during the peak weeks of a community outbreak, with lower rates of absenteeism during the weeks before and after the peak. Certain public health measures (closing schools, quarantining household contacts of infected individuals) are likely to increase rates of absenteeism.
- Multiple waves (periods during which community outbreaks occur across the country) of illness are likely to occur with each wave lasting two to three months. Historically, the largest waves have occurred in the fall and winter, but the seasonality of a pandemic cannot be predicted with certainty.
- The court will follow applicable public health orders and safety guidance as part of its duty to maintain a safe working environment for public and staff. As a result, the court may need to enact or modify safety rules for all building occupants to mitigate virus exposure.

[Link to Template](#) (Copy and paste the text from Table 3-3C above into the corresponding Table 3-3C in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Table 3-3D: Readiness and Preparedness of Operations for Pandemic Events

The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.

Readiness and Preparedness

- Ensure telework policy is updated and those authorized to telework have tested equipment at home.
- Procure additional IT equipment (laptops, computers, peripherals, video cameras etc.) to support increased telework.
- Provide refresher training for staff/judges on videoconferencing technology.
- Review cybersecurity protocols for potential influx of telework judges/staff.
- Ensure guidelines and standards for virtual courtrooms are updated.
- Ensure appropriate amount of telework licenses to support essential functions.
- Ensure staff/judges contact information is up to date in mass notification system.
- Coordinate with local public health agencies on isolation/quarantine orders. Determine if public health will need to work with court to require isolation/quarantine orders depending on how wide transmission has spread within the community.
- Develop exposure response protocol for when court staff/judge tests positive for virus and how internal contact tracing will occur.
- Set up a dedicated webpage on the public website which will feature the court's pandemic response efforts.

[Link to Template](#) (Copy and paste the text from Table 3-3D above into the corresponding Table 3-3D in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PANDEMIC ANNEX PART B: ACTIVATION

Table 3-3E: Activation of COOP for Pandemic Events

The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.

Activation

- Activation of this annex and court COOP plan will result when local, state or federal officials declare a public health emergency.
- Activate the court's Crisis Management Team.
- Activate the Court's Emergency Operations Center using virtual meeting options.
- Establish contact with appropriate local health officials to provide guidance and advice to the CMT.
- Communicate to judges/staff on who will be required to report to the courthouse and who will be working remotely.
- Meet with justice partners to discuss what court hearings will continue.
- Obtain an emergency order from the court of last resort.
- Communicate to public/jurors what court operations are available and what operations are postponed.

[Link to Template](#) (Copy and paste the text from Table 3-3E above into the corresponding Table 3-3E in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PANDEMIC ANNEX PART C: ONGOING COOP OPERATIONS

Table 3-3F: Ongoing Operational Response During Pandemic Events	
The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.	
Ongoing Response	
<input type="checkbox"/> Identify methods to limit the number of personnel entering the courthouse. Consider implementing virtual triage desks outside the courthouse to regulate who can enter and where to redirect public. <input type="checkbox"/> Update public website to reflect changes in court operations. <input type="checkbox"/> Maintain ongoing communications with local health department officials regarding public health guidelines and recommendations as they can change quickly. <input type="checkbox"/> As pandemic response will be ongoing, management should conduct regular check in with staff/supervisors to gauge morale and areas of concern. <input type="checkbox"/> Court Crisis Management Team will meet monthly to provide departmental updates on response and address any outstanding issues/concerns.	
Ongoing Department Specific Responsibilities in a Pandemic	
Operations	<input type="checkbox"/> Implement live stream hearings where feasible to limit persons entering inside the courthouse. <input type="checkbox"/> Court should establish criteria that will provide clear guidance on when an in-person hearing will be held. Virtual hearings will be utilized whenever possible. <input type="checkbox"/> Set recurring meetings with justice partners and local bar associations on the status of court operations. <input type="checkbox"/> Coordinate with sheriff's office to determine how in-custody hearings can appear virtually from the jail and how in-custody transportation will function in the pandemic. <input type="checkbox"/> Coordinate with IT to implement solutions to provide court services to the public through virtual modalities.
General Counsel	<input type="checkbox"/> Seek updated pandemic related emergency orders from the court of last resort.
Human Resources	<input type="checkbox"/> Assist all court departments in implementing flexible/staggered work and telework schedules to reduce the number of people in courthouse at any single time. <input type="checkbox"/> Develop sick/leave policies as needed. Implement policies on how to respond to ill employees who may have been infected by the virus. <input type="checkbox"/> Assess if onsite virus testing can be provided to judges/staff.
IT	<input type="checkbox"/> Maximize video conferencing options for all active courtrooms. <input type="checkbox"/> Expand bandwidth to allow for telework surge. <input type="checkbox"/> Provide technical support to all judges/staff working remotely. <input type="checkbox"/> Maintain heightened cybersecurity posture as more judges/staff are working remotely.
Facilities	<input type="checkbox"/> Maintain pandemic related signage at all courthouse entrances. <input type="checkbox"/> Social distancing markers should be placed in all public and secure areas. <input type="checkbox"/> Deploy hand sanitizing stations throughout all high traffic areas.

[Link to Template](#) (Copy and paste the text from Table 3-3F above into the corresponding Table 3-3F in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

Table 3-3G: Safety Measures to be Provided During a Pandemic

The following are safety measures to protect judges/staff and ensure safe courthouses during a pandemic.

Facilities

- Provide social distancing spacing/markers throughout courthouse as recommended by public health officials.
- Ensure pandemic related signage is easy to understand, utilizes a mix of pictures/words, and is accessible in multiple languages.
- Provide plexiglass or other barriers for judges/staff in conjunction with social distancing.
- Assess HVAC airflow and prioritize intake of outside air versus recycling interior air.
- Install hand sanitizing stations through high trafficked areas.
- Increase cleaning throughout the courthouse. Verify all cleaning products are registered with the EPA and known to kill the virus.

Safety Protocols

- Consider if face covering policy is needed for occupants working inside the court and anyone visiting the court.
- Consider rules on who can be excluded from the courthouse if ill or exposed to the virus.
- Consider limiting all In-person meetings and other gatherings.
- Interpreters should leverage headsets or other forms of wireless equipment as much as possible to limit close interactions with the public.

Personal Protective Equipment

- Obtain contract with external vendor to implement temperature or symptomology screening for all those entering the courthouse.
- Procure reusable face coverings for staff/judges reporting onsite.
- Procure disposable face coverings for public entering the courthouse.
- Procure disposable gloves as needed.
- Procure additional headsets or wireless equipment for interpreters as needed.

[Link to Template](#) (Copy and paste the text from Table 3-3G above into the corresponding Table 3-3G in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

PANDEMIC ANNEX PART D: RECONSTITUTION TO NORMAL OPERATIONS

Table 3-3H: Reconstitution of Operations in a Pandemic

The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.

Reconstitution Back to Normal Operations

- Develop communication plan on how services will be fully restored back to normal operations.
- Coordinate with local health department on when court staff/judges can receive vaccination or prophylaxis.
- Develop strategy to resolve backlog in applicable case types.
- Communicate what the court is doing to resume jury trials, the safety measures the court has implemented, and what potential jurors need to know.
- Prepare courtrooms and jury deliberation rooms to safely accommodate jurors.

[Link to Template](#) (Copy and paste the text from Table 3-3H above into the corresponding Table 3-3H in the Template and then edit/complete the language in the Template table as appropriate for your court. Use link to toggle back and forth between the tables in Section II of the Guide and the corresponding tables in the Template.)

ADDITIONAL RESOURCES

National Center for State Courts (NCSC)

- [Emergency Planning and Security](#)

Federal Emergency Management Agency (FEMA)

- [Exercises](#)
- [Emergency Management Institute](#)
- [National Continuity Programs](#)
- [Continuity Resources and Technical Assistance](#)
- [Continuity Resource Toolkit](#)
- [COOP Training](#)
- [Ready Business](#)

Communication Resources

- [Government Emergency Telecommunications Service](#)
- [Wireless Priority Service](#)
- [Telecommunications Service Priority](#)
- [FirstNet](#)

APPENDIX: COOP TEMPLATE

Continuity of Operations (COOP) Plan

[Insert Name of Court]

[Insert Effective Date]

[Insert Court Seal or other Graphic]

COOP TEMPLATE - PART A: READINESS AND PREPAREDNESS

PURPOSE

Table 2-1: Purpose of the Court's COOP Plan

--

[Back to Guide](#)

APPLICABILITY AND SCOPE

Table 2-2: Applicability and Scope

--

[Back to Guide](#)

DISTRIBUTION AND MAINTENANCE OF PLAN

Table 2-3A: Revision Control

Date	Summary of changes	By Whom

[Back to Guide](#)

Table 2-3B: Plan Maintenance

Where will physical copies of the COOP be located?	
Where will virtual copies of the COOP be located?	
Intended audience for this plan.	
Person responsible for maintaining the overall COOP.	
How often will this plan be maintained?	
Protocol for ensuring updates/revisions to this COOP are made for both physical and virtual versions.	
<i>Insert others</i>	

[Back to Guide](#)

CRISIS MANAGEMENT TEAM (CMT)

The CMT will consist of those in an overarching policy/executive body which governs and directs policy related to crisis response for all courthouses within a court system. Similarly, there is a designation of those who have crisis management functions at a local courthouse level (e.g., Courthouse Unified Command Team)

- Policy Group – Policy Group serves as a decision-making authority helping direct the priorities in an incident. This group decides major policy decisions such as closing a courthouse, decides when to send court staff home, determines court wide communication message, provides the courts statement to the press, etc.
- Local Court Unified Command Team – A Unified Command Team will help direct incident response at their specific courthouse. They help provide quick emergency actions that take place at a single courthouse location.

Table 2-4: Crisis Management Team (CMT)	
CMT	Members of the Team
COOP Coordinator	
Backup COOP Coordinator	
Policy Group	
Courthouse Unified Command Team – insert courthouse	
Courthouse Unified Command Team – insert courthouse	
Insert others	

[Back to Guide](#)

COURT EMERGENCY OPERATIONS CENTER (EOC) AND MEETING LOCATIONS

Table 2-5: Meeting Locations		
Physical Meeting Options		
Courthouse	Inside Meeting Area	Outside Meeting Area
Virtual Meeting Options		
Virtual Modality	Protocols to Access	Any Restrictions

[Back to Guide](#)

COURT ESSENTIAL FUNCTIONS

Table 2-6 contains a listing of the court’s most time-critical and essential functions that cannot be left undone for 30 days without risking failure of mission, failure meeting of statutory/mandatory obligations, or loss of trust, respect, and funding. Each table represents a court essential function. Table 2-7 contains a Business Impact Analysis (BIA) and can be included as an attachment to the COOP plan.

Table 2-6: Essential Functions (EFs) - Business Impact Analysis Worksheet (Complete separate Table for each court department and include as Attachment to COOP Plan)			
Department: (Insert Department)			
Critical Activity/Essential Function (EF)	Priority	Impact if EF is not completed	Return Time Objective
(Add additional rows as needed)			

[Back to Guide](#)

Table 2-7: Essential Functions (EFs) - Business Process Analysis				
Essential Function	Recovery Time Objective	Department/Person Responsible	Key Staff	
(Essential Function #1)	Resources Needed			
	Work Location & Space Requirements			
	Supporting Activities			
	Internal Dependencies/Essential Records			
	External Dependencies/Essential Records			
	Manual Workarounds			
	Related Regulation			
	Can an Emergency Order provide relief?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Notes:
	Can EF be done via telework?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Notes:

[Back to Guide](#)

TECHNOLOGY CONSIDERATIONS – ESSENTIAL RECORDS, COURT APPLICATIONS, NETWORK

Table 2-8A: Technology Priorities				
IT Application/Vital Record	Return Time Objective (RTO)	Recovery Point Objective (RPO)	Unit Responsible/Point of Contact	Notes

[Back to Guide](#)

Table 2-8B: Telework Logistics	
Item to Consider	Explanation, Response, or Protocol
How many telework (VPN) licenses does the court maintain?	
Does the court have a current policy on how telework will be used in a crisis?	
What IT cybersecurity protocols need to be in place to implement emergency telework?	
What will be the plan to surge telework options (e.g., purchase new laptops, reuse existing computers)?	
What changes need to be made to the court network or infrastructure to support expanded telework?	
How will telework capabilities be tested prior to an emergency	
How will telework equipment be deployed to judges/staff?	
How is bandwidth addressed for critical applications to be used offsite or at an alternate facility?	
Are there any court applications, software, or programs that can't be accessed offsite?	
What type of ergonomic protocols need to be in place for telework to prevent injuries?	
How will employee privacy be maintained during telework?	

[Back to Guide](#)

ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

Table 2-9: Orders of Succession and Delegations of Authority				
Key Position	Successor	Delegated Authority	Activation/Termination of Delegated Authority(s)	Resources Needed
<i>Insert key position</i>	<i>Successor 1</i>			
	<i>Successor 2</i>			
	<i>Successor 3</i>			
<i>(Include as many additional rows as necessary)</i>				

[Back to Guide](#)

ALTERNATE FACILITIES AND GO KITS

In the event a courthouse is non-operational, there will be a need to ensure the continuation of the court's essential functions offsite. Table 2-10A provides guidance and a checklist to help the court identify potential alternate facility sites and can be included as an attachment to the court's COOP plan. Sites should be evaluated before an emergency and potential sites are listed on a chart on the following page.

Table 2-10A: Alternate Facility Evaluation Checklist

Alternate Facility Criteria	Comments
Physical Layout	
Where is the facility located?	
How much floor space does the facility have?	
Can the rooms be partitioned? Is the available floor space contiguous or on different floors/in different wings?	
How many staff workstations can the facility accommodate?	
How many courtrooms can the facility accommodate?	
Does the facility have electricity, backup generator, and available power outlets?	
Does the facility have desks, chairs, and other furniture needed for setup?	
Are any private offices available? Any rooms that could be used as judicial chambers?	
Are there break rooms available for staff?	
Are restrooms available for the public, staff, and judges?	
Is there available parking for staff and the public?	
How easy is it for the public to find the building? Is the building ADA accessible?	
Is the site best suited for courtrooms, case processing, office work, public counter services, etc.?	
What type of agreement (e.g., financial contract, memorandum of understanding/agreement, statutory change to allow the court to sit in another jurisdiction) is necessary to secure the facility for the court's use?	
IT Functionality	
Is the facility equipped for internet or wireless internet connectivity? Is the signal strength strong enough to support the needed IT applications?	
If using mobile hotspots, what is their signal strength? Is the signal strength strong enough to support the needed IT applications?	
What critical IT applications need to be accessed from the facility?	
What type of phone lines are available?	
Security Considerations	
Are there secure areas to lock sensitive or confidential items after hours?	
Is there a secure parking area and entry for judges?	
Are there any security vulnerabilities? (e.g., multiple entrances, no escape for judge/staff)	
If inmates are to be transported to the facility for hearings, what type of secure access will there be to get them in/out of the facility?	
How much security personnel will the facility require?	
Is there a location for a weapons screening station to be set up?	

[Back to Guide](#)

Table 2-10B: Alternate Facility Locations

Alternate Facility #1 Facility name: Address: Point of Contact:	
Expected Use (courtroom, offices, jury assembly, etc.)	
Available Utilities	
Furniture/Equipment Needed	
Wi-Fi/Network Options	
Floor space (sq.ft)	
Parking Availability	
Accessibility Concerns	
Vulnerabilities	
Agreement	
Staffing Considerations	
List potential anticipated number of judges and staff reporting to the alternate facility	
Who is responsible for judges/staff reporting to the alternate facility?	
Who provides orientation on the following topics? (break room, restrooms, parking, security, safety, emergency evacuation, supplies, card/key access)	
Who provides notification to the following entities about the alternate facility?	
Staff	
Parties/Litigants	
Justice Partners	
Public	
Alternate Facility #2 Facility name: Address: Point of Contact:	
(Add additional facilities as appropriate)	

[Back to Guide](#)

Go-Kits

When implementing an alternate facility, a court will most likely need to transport necessary supplies to ensure the continuation of that essential function. Court departments should develop Go Kits to ensure the continuation of their specific essential functions. Table 2-10D includes a sample checklist/form to help court departments in organizing their go-kit.

Table 2-10C: Go Kit Checklist (To be Included as an Attachment to COOP Plan)			
Go Kit (Department/Unit)			
Go Kit Location			
Last Checked			
Item	Pre-Staged	To Be Recovered	
	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	
(Insert items as appropriate)	<input type="checkbox"/>	<input type="checkbox"/>	

[Back to Guide](#)

EMERGENCY COMMUNICATIONS

Communication is a critical element to ensure a court can successfully continue its essential functions. The following table identifies the available communication modalities, situational awareness, and stakeholder communications.

Table 2-11A: Communication Modalities				
Communication System	Where is system located?	Who has access?	Unit responsible?	Who can receive communications?
Voice Lines				
Email				
Mobile Phones				
Mass Communication				
Two-Way Radios				
Emergency Phone Message Number				
Cloud based information site				
Videoconference Platforms				
Satellite Phones				
Social Media				
GETS/WPS				
FirstNet Devices				
Fax Lines				
Building PA systems				
<i>Insert others</i>				
<i>Insert others</i>				

[Back to Guide](#)

Table 2-11B: Communication Strategies

Situational Awareness			
How will the court maintain a Common Operating Picture (COP), so management and judicial leadership understand the situation and what the operational plan is?			
How will the court provide updates to judges/staff who may not be onsite or have access to their court email?			
How will the court communicate operational status to the local/county emergency operations center?			
Does the court have a seat at the local/county EOC?			
<i>Insert additional rows as needed</i>			
Stakeholder Communications			
Stakeholder	Primary Communicator	Frequency of Communications	Communication Modality
Staff			
Judges			
Justice Partner/Building Tenants			
Jurors			
Litigants/Witnesses/Parties			
Media			
Employee Unions			
Public			
Local/County EOC			
Sheriff's Office			
Local Bar Associations/Legal Service Associations			
State AOC			
<i>Insert others</i>			
<i>Insert others</i>			
Last Resort Plan			
In the event that all primary forms of communication are not operable, how will communication and coordination occur?			

[Back to Guide](#)

HUMAN RESOURCES CONSIDERATIONS

Table 2-12A: Workforce Contact Lists	
Item to Consider	Guidance Available
Who is responsible for collecting contact information?	
Where are rosters with all staff/judge contact information maintained?	
How often is contact information Audited?	
Procedure for handling staff/judge injuries, death, notification of next of kin, or other designated contacts.	
<i>Insert others</i>	

[Back to Guide](#)

Table 2-12B: Employee Welfare and Staffing Strategies	
Item to Consider	Guidance Available
Employee Welfare	
What services are available to help employee welfare during a crisis?	
How will disaster fatigue be addressed?	
<i>Insert others</i>	
Staffing Strategies	
Procedure for hiring additional staff on an interim basis (e.g., temp agencies, retirees, etc.)	
Procedure for on how to obtain additional judges if there is a shortage of judicial officers available.	
<i>Insert others</i>	

[Back to Guide](#)

Table 2-12C: HR Policies and Guidance		
Personnel Areas	Specific Personnel Issue	Guidance Available
Work schedules and compensation	Payment of nonessential staff	
	Role of nonessential staff	
	Overtime for essential functions staff	
	Payroll administration when normal processes unavailable	
	<i>Include additional issues here</i>	
Flexible work hours	Modification of work hours	
	<i>Include additional rows as needed</i>	
Leave	Emergency leave	
	<i>Include additional rows as needed</i>	
Obtaining additional staff	Emergency staffing	
	<i>Include additional rows as needed</i>	
Logistical support	Emergency housing	
	<i>Include additional rows as needed</i>	
Discipline	Employee Discipline	
	<i>Include additional rows as needed</i>	
Education and training	Preparedness Training	
	<i>Include additional rows as needed</i>	
Telework	Telecommuting	
	<i>Include additional rows as needed</i>	
Other		
	<i>Include additional rows as needed</i>	

[Back to Guide](#)

RESOURCE MANAGEMENT

Table 2-13: Resource Management Strategy	
Item to Consider	Explanation, Response, or Protocol
How will emergency purchases be made? Who will take the lead in procuring and managing supplies in an emergency?	
Which positions have access to court credit cards that can be used in an emergency? What is their limit?	
What is the protocol for requesting resources from the local/county emergency operations center? What resources are they able to provide in an emergency?	
What is the protocol for requesting resources from the State AOC? What resources are they able to provide in an emergency?	
Where is the list of critical vendors and contact information maintained? Who maintains it?	
Have all courthouses been designated with priority utility service and for priority restoration after a disaster? Where are the emergency contacts for each utility stored?	
What is the protocol to ensure courthouse generators (if applicable) are maintained and refueled during an emergency?	
How long does each courthouse generator run, and what will it power?	
What mutual aid agreements are in place with other court systems to provide aid in an emergency? What resources can be provided or shared?	
Where are court emergency supplies stored and maintained? (e.g., food, water, first aid, flashlights, dust masks, USB chargers, laptop power banks, etc.)? Include any hazard-specific emergency supplies.	
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Back to Guide](#)

DEVOLUTION

The court's devolution plan describes what to do if a catastrophic event renders the court's leadership and essential functions staff incapacitated and the court and alternate facilities nonfunctional. During devolution, the court transfers authority and responsibility for essential functions to officials in another court.

Table 2-14: Devolution Plan

Table 2-14: Devolution Plan		
Provide contact information for the alternate court(s) available to perform essential functions (Add as many rows as necessary)		
Court	Contact Information	Is there a written agreement with the alternate court(s)?
		<input type="checkbox"/> Yes <input type="checkbox"/> No
		<input type="checkbox"/> Yes <input type="checkbox"/> No
List the officials and their successors (by position) allowed to transfer authority to perform essential functions (Add as many rows as necessary)		
Succession	Title	
Primary Official		
Successor		
Successor		
Provide plan for transferring essential records and other materials necessary for performing essential functions to alternate court(s). For example, will essential records and materials be stored and updated on the same schedule as those stored with alternate facilities?		
List procedures for notifying the alternate court of devolution.		
<input type="checkbox"/>		
<input type="checkbox"/> <i>Insert items as appropriate</i>		
List procedures for returning authority once court is reconstituted.		
<input type="checkbox"/>		
<input type="checkbox"/> <i>Insert items as appropriate</i>		
Are there any essential functions that are unable to be transferred to another court system due to law, regulation, or statute?		
<input type="checkbox"/>		
<input type="checkbox"/> <i>Insert items as appropriate</i>		

[Back to Guide](#)

COOP TEMPLATE - PART B: ACTIVATING COOP IN A DISASTER

COOP ACTIVATION

The following are considerations to aid the court in determining if it will activate the COOP. Not every emergency requires activation of the COOP. Some emergencies may require a short-term evacuation of the court facility followed by the resumption of normal operations. COOP response should be flexible and scalable based on the emergency incident.

Table 2-15A: COOP Activation Considerations	
General Considerations For When to Activate the COOP	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Questions to Assess COOP Activation Trigger Points	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Note: * indicates events occurring after work hours; ** indicates events occurring without warning	

[Back to Guide](#)

Table 2-15B: COOP Activation Checklist	
Initial Status Briefing, Assessment, and COOP Activation	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Crisis Management Team Activation	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Department Managers Activation	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Other Key Stakeholders Activation	
<input type="checkbox"/>	
<input type="checkbox"/>	<i>Insert items as appropriate</i>

[Back to Guide](#)

COOP TEMPLATE - PART C: ONGOING COOP OPERATIONS DURING EMERGENCIES

KEY ROLES/RESPONSIBILITIES OF COURT DEPARTMENTS DURING A CONTINUITY EVENT

Table 2-16: Key roles/responsibilities during a continuity event	
COOP Coordinator/Emergency Management	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Court Operations	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Finance	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
IT	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Human Resources	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
General/Legal Counsel	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Facilities	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Public Information Officer	
<input type="checkbox"/>	<i>Insert items as appropriate</i>
Insert other departments as necessary	
<input type="checkbox"/>	<i>Insert items as appropriate</i>

[Back to Guide](#)

COOP TEMPLATE - PART D: RECONSTITUTION AND COST RECOVERY

RECONSTITUTION

Reconstitution includes procedures to terminate alternate operations and resume normal operations. The reconstitution information in the table below provides a plan to return to normal operations once the CMT determines the disaster no longer poses a threat. Reconstitution is not a single point in time event but rather a planning process that involves consideration of how to restore operations at the courthouse.

Table 2-17A: Reconstitution Team Responsibilities	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	Insert items as appropriate

[Back to Guide](#)

Table 2-17B: Reconstitution Logistics	
Item to Consider	Explanation, Response, or Protocol
Who will comprise the Court's Reconstitution Team?	
Who will oversee leading the Reconstitution Team?	
What initial assessment is done for reconstitution?	
Who is responsible for developing communication to the various court stakeholders during the reconstitution process?	
What is the role of the State AOC during reconstitution?	
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Back to Guide](#)

COST RECOVERY

Table 2-18: Cost Recovery Logistics	
Item to Consider	Explanation, Response, or Protocol
Who will comprise the court's Cost Recovery Team?	
Who will oversee leading the Cost Recovery Team?	
What job code (or other mechanism) will be used to track services, supplies, and personnel costs associated with the emergency?	
Which entity is responsible for applying for FEMA Public Assistance (Court, AOC, County Emergency Management, etc.)?	
What is the overall process by which the Court will track and submit costs during an emergency and ensure FEMA procurement rules are followed?	
How are the courthouses currently insured? Where are the insurance documents located?	
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Back to Guide](#)

AFTER-ACTION REVIEWS

At the conclusion of every COOP activation, an after-action report with a corrective action plan will be completed. This AAR will assist the court in further enhancing its emergency planning and response.

Table 2-19: After-Action Review

Item to Consider	Explanation, Response, or Protocol
Who will be responsible for leading the after-action review after an emergency incident?	
What methodology will be used to develop an AAR? (e.g., surveys, meetings, one on one interviews)	
How quickly will a written AAR be developed following the conclusion of an emergency incident?	
A written copy of the AAR will be distributed to the following stakeholders.	
Each of the following areas will be evaluated during an AAR.	
A Correction Action Plan (CAP) will be developed to capture action items learned from the AAR. Who will be responsible for ensuring the items listed in the CAP are implemented?	
Where will completed after-action reports reside?	
<i>Insert other questions to cover any additional procedures the court wishes to specify for this topic.</i>	

[Back to Guide](#)

COOP TRAINING AND EXERCISE PROGRAM IDENTIFICATION WORKSHEET

Table 3-1: COOP Training and Exercise Program Identification Worksheet

Type of Training	Recipients	Method(s)	Frequency
COOP Orientation			
COOP Refresher			
Updates to FEMA Cost Recovery Process			
<i>Insert others</i>			
Exercises			
Type of Exercise	Recipients	Method(s)	Frequency
Drill			
Tabletop			
Functional			
Full Scale			
<i>Insert others</i>			

[Back to Guide](#)

COOP HAZARD ANALYSIS WORKSHEET

Table 3-2: Hazard Analysis						
Scoring Factor	Hazard					
	<i>Insert hazard</i>					
Probability (1-5) One means low probability of occurrence and five meaning a high probability of occurrence.						
Severity (1-5) One means low impact to court functions and five meaning a critical impact to court operations.						
Total Risk (P x S) Multiply probability by severity to attain total risk score.						

[Back to Guide](#)

COOP HAZARD ANNEX TEMPLATE

PANDEMIC ANNEX PART A: READINESS AND PREPAREDNESS

Table 3-3A: Purpose of (Insert Hazard) Annex

[Back to Guide](#)

Table 3-3B: Continuity Objectives for (Insert Hazard)

The overarching objectives in a (insert hazard) include:

- (Insert objectives)
-

[Back to Guide](#)

Table 3-3C: COOP Planning Assumptions for (Insert Hazard)

The following are typical assumptions the court may face in a (insert hazard) incident:

- (Insert assumptions)
-

[Back to Guide](#)

Table 3-3D: Readiness and Preparedness of Operations for (Insert Hazard)

The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.

Readiness and Preparedness

- Insert items as appropriate*
-

[Back to Guide](#)

PANDEMIC ANNEX PART B: ACTIVATION

Table 3-3E: Activation of COOP for (Insert Hazard)

The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.

Activation

- Insert items as appropriate*
-

[Back to Guide](#)

PANDEMIC ANNEX PART C: ONGOING COOP OPERATIONS

Table 3-3F: Ongoing Operational Response During (Insert Hazard)	
The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.	
Ongoing Response	
<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>	
Ongoing Department Specific Responsibilities in a Pandemic	
Operations	<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>
General Counsel	<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>
Human Resources	<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>
IT	<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>
Facilities	<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>

[Back to Guide](#)

Table 3-3G: Safety Measures to be Provided During (Insert Hazard)	
The following are safety measures to protect judges/staff and ensure safe courthouses during a pandemic.	
Facilities	
<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>	
Safety Protocols	
<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>	
Personal Protective Equipment	
<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>	

[Back to Guide](#)

PANDEMIC ANNEX PART D: RECONSTITUTION TO NORMAL OPERATIONS

Table 3-3H: Reconstitution of Operations in a Pandemic	
The following are action steps designed to assist the court in a pandemic incident. These action steps are meant to supplement the existing protocols and actions developed in the Court's COOP plan due to the unique pandemic hazard.	
Reconstitution Back to Normal Operations	
<input type="checkbox"/> <i>Insert items as appropriate</i> <input type="checkbox"/>	

[Back to Guide](#)

DV AWARE
Collaboration Multiplier

Goal: Identify Partners for Successful Collaboration on Analysis & Warning

Sectors/Partners*	Expertise*	Assets/Strengths*	Roles/Resources*	Key Strategies*

*Sectors/Partners: Identify those key stakeholders needed for Analysis and Warning planning and implementation, including but not limited to government agencies, community organizations, culturally-specific organizations, victim-centered organizations, faith-based organizations, etc.

*Expertise: What unique expertise does this field bring to the collaborative?

*Assets/Strengths: What resources (skills, staff, training capacity, funding) can be brought to the table?

*Roles/Resources: What role will the partner play and what resources can they bring to the collaborative?

*Key Strategies: What key strategies/activities are currently implemented relevant to this issue?

COURT MAPPING - ACTION

Locations in, Around or Near the Courthouse

- Parking lot
- Entry security
- Clerk's office
- Court services
- Interpretation
- Self-help
- Courtroom
- Parent education
- Mediation/ADR
- DV Program
- Attorney's office
- Child custody evaluation
- Parenting coordination
- Guardian ad Litem office
- Mental health provider's office
- Child protection office
- Safe visitation exchange location

COURT MAPPING - ACTION

Court Case Events

- Filings
- Service
- Mediation/ADR
- Protective order hearing
- Temporary hearing
- Default hearing
- Arraignment/preliminary hearing
- Bail/release hearing
- Probation meeting
- Status conference
- Final trial
- Post-trial motions
- Post-decision review hearing
- Settlement conference
- Pre-trial conference
- Final judgement/verdict
- Waiting area(s)
- Evaluations
- Parenting classes
- Batterer's intervention
- Advocate meeting
- Attorney-client meeting
- Safe visitation exchange
- Judge in chambers

COURT MAPPING - ACTION

Court System-Related Persons

- Victim/Survivor
- Abuser
- Children
- Extended family
- Witnesses
- Judge
- Court commissioner/referee
- Court clerk
- Self-help staff
- Court security officer
- Bailiff
- Law enforcement officers
- Front desk clerk
- Mediator/ADR provider
- Custody evaluator
- GAL
- Parenting coordinator
- Attorney
- DV advocate
- CPS
- Supervised visitation and exchange provider
- Mental health provider
- Probation/Parole

DV AWARE
Collaboration Multiplier

Goal: Identify Partners for Successful Collaboration on Action

Sectors/Partners*	Expertise*	Assets/Strengths*	Roles/Resources*	Key Strategies*

*Sectors/Partners: refer to those key stakeholders needed Action planning and implementation, including but not limited to government agencies, community organizations, culturally-specific organizations, victim-centered organizations, faith-based organizations, etc.

*Expertise: What unique expertise does this field bring to the collaborative?

*Assets/Strengths: What resources (skills, staff, training capacity, funding) can be brought to the table?

*Roles/Resources: What role will the partner play and what resources can they bring to the collaborative?

*Key Strategies: What key strategies/activities are currently implemented relevant to this issue?

EMERGENCY ACTION PREPAREDNESS

This activity will provide opportunities for determining the extent of emergency preparedness already underway and for assessing which functions other staff members and agencies perform that may assist the court in developing or enhancing its emergency action planning.

SCENARIO

You have the same job you normally hold, either in the courthouse or in the community. While you are in the court building on a lunch break in the cafeteria/food cart, you hear what sounds like firecrackers popping. Everyone in the area begins mumbling and looking for the source of the sound. You get an uneasy feeling and you hear the people around you ask, "what was that?" Before too long, someone opens a door and shares that a disgruntled former defendant is in the courthouse with a firearm. He is moving from the entrance to the courtrooms. The person then ask you what should be done.

INDIVIDUAL QUESTIONS

Describe the actions you would take and the directions you would provide given your current position.

What are your responsibilities in a situation like this?

Based on your responsibilities what do you do first, second, third, etc.?

1. _____
2. _____
3. _____
4. _____

EMERGENCY ACTION PREPAREDNESS

5. _____

Who do you contact first, second, third, etc.? How do you contact them?

1. _____

2. _____

3. _____

4. _____

5. _____

GROUP QUESTIONS

What are your thoughts about the adequacy of your courthouse's current emergency plans for dealing with this and other types of emergencies?

What recommendations do you have that might enhance current emergency plans?

Other Trauma-Responsive Practice Resources

<https://www.pacesconnection.com/g/resource-center/blog/resource-list-topic-trauma-informed-practice>

<https://dvrisc.org/community-readiness-toolkit-overview/>

<https://www.ovcttac.gov/taskforceguide/eguide/6-the-role-of-courts/63-trauma-informed-courts/>

<https://www.ncjfcj.org/child-welfare-and-juvenile-law/trauma-informed-courts/>



Are We Trauma-Informed?

Tools to Measure Progress in a Program, School, or Organization



Interest in trauma-informed approaches across child-serving systems has surged in the past two decades. This interest has largely been in response to research showing that most children experience at least one potentially traumatic event by the age of 17 years,¹ together with the strong relation between childhood trauma exposure and problems with health, mental health, and other concerns across the life span.² Trauma-informed approaches integrate understanding of trauma throughout a program, organization, or system to enhance the quality and scope of services for those affected by trauma.³ However, there is a lack of research on how to measure and evaluate a trauma-informed approach. How do staff measure the extent to which a program, school, or organization is trauma-informed? How do managers/leaders know whether the trauma-informed efforts of their programs, schools, or organizations are effective in promoting thriving among children, families, and staff?

Defining Key Components of a Trauma-Informed Approach

Although there is variation in how a “trauma-informed approach” is defined, one review⁴ identified 15 common

components that can be organized into three categories. In order to determine whether an initiative is trauma-informed, it is important to assess these components:

1. **Workforce development** involves promoting knowledge of trauma (for instance, through staff trainings and a healthy workforce).
2. **Trauma-focused services** include screening and access to trauma-focused interventions.
3. **Organizational environment and practices** include policies and practices that promote trauma-related communication and collaboration.

Reviewing Measures of a Trauma-Informed Approach

Researchers from CHDI, the Yale School of Medicine, and the Medical University of South Carolina conducted a [systematic review⁵ of measures](#) (in particular, surveys) of a trauma-informed approach that were published between 1988 and 2018. Using specific search terms, the research team reviewed journal articles and websites for surveys that measured a systems-level, trauma-informed approach focused on addressing psychological trauma. The paper did not include trauma screening tools or diagnostic measures.

The systematic review includes **49 surveys** of a trauma-informed approach. Characteristics of each survey were identified and summarized, including length, relevant context, components of a trauma-informed approach assessed, research support, and cost. Whereas some of the surveys were applicable to a wide range of contexts, others were developed to assess policies and practices within specific settings. Four examined approaches focused on improving family and other relational processes; 38 examined approaches in organizations, including schools and health settings; and seven assessed approaches that involved a whole community or service system. Forty-two of the surveys examined workforce development, 24 examined trauma-focused services, and/or 23 examined organizational environment and practices. Twelve surveys examined all three domains. In general, most surveys had little research support in regard to their development and application in practice. The team found only one study that examined whether survey scores (i.e., on the Trauma-Informed Practice Scales) were related to improvements in service recipients' general health and well-being (e.g., self-efficacy).^{6,7} The remaining surveys varied in the extent to which they had research support. For instance, not all of the surveys had performance statistics; validity statistics reflect the extent to which a survey measures what it is intended to measure and reliability statistics indicate the extent to which a survey performs consistently. The best surveys should have evidence of both validity and reliability.

Examples of Promising Surveys

Table 1 below includes information on four surveys from the review. These surveys were selected by the research team as promising tools for assessing a trauma-informed approach, each of which has some research support.

Table 1. Examples of Promising Surveys of a Trauma-Informed Approach

Measure	# of items	Context(s)					Component(s)			Cost
		Family	Education	Child Welfare	Health	Other	Workforce Development	Trauma-Informed Services	Organizational Environment and Practices	
Attitudes Related to Trauma-Informed Care (ARTIC) Scale ⁸	45-, 35-, and 10-item versions		x		x	x	x		x	Starts at \$500
TICOMETER ⁹	35			x	x	x	x	x		Starts at \$250
Trauma-Informed Practice (TIP) Scales ⁷	20	x				x	x	x	x	Free upon request
Trauma-Informed System Change Instrument (TISCI) ¹⁰	19		x	x	x	x	x	x	x	Free online

Measuring or Evaluating Trauma-Informed Approaches

Measuring a trauma-informed approach can help to increase provider understanding of trauma, inform prioritization of implementation strategies, and be used to assess changes during implementation. As part of its efforts to help improve the quality of, and access to, children's mental health services in Connecticut, CHDI has partnered with the Connecticut Department of Children and Families and the Court Support Services Division of the Judicial Branch in using the TISCI¹⁰ and

similar measures to assess the degree to which [child welfare](#) and juvenile justice policies and procedures were trauma-informed and contributed to modifications of [policies](#) and practice guides to better address childhood trauma.

The following recommendations are for organizations, programs, or systems that are also interested in assessing the extent to which they are trauma-informed:

- Consider using a survey that shows promise based on its performance statistics (e.g. validity and reliability).
- Consider characteristics of the survey, including length, cost, and available languages and, based on this information, whether this survey will be feasible to implement and accessible to diverse participants.
- Explore how to adapt existing surveys that may have some research support rather than develop new tools that are only intended to evaluate a specific program.
- In selecting a survey, consider the specific question(s) that will be addressed. For example, is it more important to perform an organizational needs assessment, or examine the potential impacts of a practice or policy on staff knowledge and skills? How will survey results be used?

Advancing Research on Trauma-Informed Approaches

Measures (e.g., surveys) of a trauma-informed approach offer opportunities to examine whether programs, organizations, and broader service systems can support the health of those affected by trauma. Stakeholders need effective measures to identify their strengths and areas for improvement and to monitor their progress toward becoming trauma-informed. Although the larger review identified 49 promising surveys, more work is needed to provide a stronger evidence base, including developing reliable and valid surveys that are applicable across various service systems. In addition, research is needed to determine the extent to which changes in a trauma-informed approach contribute to improvements in child and family outcomes, which is the ultimate goal of a trauma-informed approach.

REFERENCES

1. Finkelhor, D., Turner, H. A., Shattuck, A., & Hamby, S. L. (2013). Violence, crime, and abuse exposure in a national sample of children and youth: An update. *JAMA Pediatrics*, *167*(7), 614-621.
2. Felitti, V. J., Anda, R. F., Nordenberg, D., Williamson, D. F., Spitz, A. M., Edwards, V., ...Marks, J. S. (1998). Relationship of childhood abuse and household dysfunction to many of the leading causes of death in adults. The Adverse Childhood Experiences (ACE) Study. *American Journal of Preventive Medicine*, *14*(4), 245-258.
3. SAMHSA's concept of trauma and guidance for a trauma-informed approach. (2014). Substance Abuse and Mental Health Services Administration. Retrieved from: <https://store.samhsa.gov/shin/content/SMA14-4884/SMA14-4884.pdf>
4. Hanson, R. F., & Lang, J. (2016). A critical look at trauma-informed care among agencies and systems serving maltreated youth and their families. *Child Maltreatment*, *21*(2), 95-100.
5. Champine, R. B., Lang, J., Nelson, A. M., Hanson, R. F., & Tebes, J. K. (2019). Systems measures of a trauma-informed approach: A systematic review. *American Journal of Community Psychology*. (in press)
6. Sullivan, C. M., Virden, T., Strom, J., Goodman, L. A., & Ramirez, R. (2018). Evaluation of the effects of receiving trauma-informed practices on domestic violence shelter residents. *American Journal of Orthopsychiatry*, *88*(5), 563-570.
7. Goodman, L. A., Sullivan, C. M., Serrata, J., Perilla, J., Wilson, J. M., Fauci, J. E., & DiGiovanni, C. D. (2016). Development and validation of the Trauma-Informed Practice Scales. *Journal of Community Psychology*, *44*(6), 747-764.
8. Baker, C. N., Brown, S. M., Wilcox, P. D., Overstreet, S., & Arora, P. (2016). Development and psychometric evaluation of the Attitudes Related to Trauma-Informed Care (ARTIC) Scale. *School Mental Health*, *8*(1), 61-76.
9. Bassuk, E. L., Unick, G. J., Paquette, K., & Richard, M. K. (2017). Developing an instrument to measure organizational trauma-informed care in human services: The TICOMETER. *Psychology of Violence*, *7*(1), 150-157.
10. Richardson, M. M., Coryn, C. L. S., Henry, J., Black-Pond, C., & Unrau, Y. (2012). Development and evaluation of the Trauma-Informed System Change Instrument: Factorial validity and implications for use. *Child and Adolescent Social Work Journal*, *29*(3), 167-184.

This Issue Brief was prepared by Robey B. Champine, PhD, MS, MPH, former Postdoctoral Fellow at CHDI and current Assistant Professor of Public Health at the Michigan State University College of Human Medicine; Ashley M. Nelson, Senior Data Analyst at CHDI; and Jason M. Lang, PhD, Vice President for Mental Health Initiatives at CHDI. For more information, contact Dr. Champine at champi74@msu.edu or visit www.chdi.org.

ORGANIZATIONAL SELF-ASSESSMENT: ADOPTION OF TRAUMA-INFORMED CARE PRACTICE

The Organizational Self-Assessment is designed for organizations interested in improving their policies, procedures, practices and social and physical environment to reflect the core principles and values of a trauma-informed care organization. It is designed primarily as a performance improvement resource to increase an organization's awareness of the key components of a trauma-informed care organization and to engage in a self-reflective process that assists them in identifying what they need to: 1) **keep** doing and reinforcing, 2) **stop** doing and, 3) **start** doing, in order to advance their efforts to become a continually improving trauma-informed care organization.

The Organizational Self-Assessment instrument consists of six (6) trauma-informed care domains, characteristic of a trauma-informed care organization, along with a set of performance standards for each. These domains and standards reflect a compilation of commonly recognized aspects of a trauma-informed care organization, influenced by the work of leaders in the field. A seventh domain was added to assist an organization in assessing its readiness to measure and evaluate performance improvement. It is recommended that the Organizational Self-Assessment be independently completed by a range of stakeholders including; leadership, supervisors, practitioners, consumers, and support staff. This will ensure a comprehensive assessment of the organization from a broad perspective.

The domains and standards were designed to reflect the following core values and principles of trauma informed care:

A Trauma-Informed Care Organization Includes:

Safe, calm and secure environment with supportive care

System wide understanding of trauma prevalence, impact and trauma informed care

Cultural Competence

Consumer voice, choice and self-advocacy

Recovery, consumer-driven and trauma specific services

Healing, hopeful, honest and trusting relationships

Indicate, as best you can, the degree to which the following standards describe your organization on a five point scale, ranging from 0 to 4:

0 = we don't meet this standard at all

1 = we minimally meet this standard

2 = we partially meet this standard

3 = we mostly meet this standard

4= we are exemplary in meeting this standard (we have much to offer other grantees)

*A score of 4 means you meet this standard very well and have expertise in this area that may be of help to other grantees interested in improving their performance around this standard.
 N/A = I am not sure I understand this question.

ORGANIZATIONAL SELF-ASSESSMENT: ADOPTION OF TRAUMA-INFORMED CARE

1. Early Screening and Comprehensive Assessment of Trauma

Performance Standards:

A. The initial (first encounter with the agency) intake, assessment and documentation process includes questions designed to sensitively and respectfully explore prior (including early childhood) and current trauma related experiences. The information gathering process enables a person to reveal personal histories and experiences at their own pace and in their own way. Exploration of trauma related experiences is done within a calm, safe, secure, and supportive setting by caring, interested, and skilled practitioners; it is never confrontational, coercive or demanding.

0 1 2 3 4 N/A

B. The organization recognizes that some consumers may not be able or willing to reveal traumatic life experiences early on in the intake/assessment process, given the sensitive nature of the topic. Procedures are in place to re-engage consumers and re-assess the issues related to trauma, for example during service plan review meetings, when new information is shared by other sources, when the consumer self-reports such information, or when warning signs are observed that are typically associated with trauma.

0 1 2 3 4 N/A

C. The screening and assessment process is sufficiently thorough and focused on trauma related issues to allow for the determination of a diagnosis associated with trauma (e.g. PTSD). The ongoing assessment process allows for the gathering of new trauma related information leading to potential changes in diagnosis as well as appropriate treatment objectives, goals, and services.

0 1 2 3 4 N/A

D. Early screening and assessment process is designed to promote shared decision-making between the consumer and the provider related to the selection of optimal services. The process involves identifying trauma related needs, strengths, and available services.

0 1 2 3 4 N/A

Comments on Domain 1: _____

2. Consumer Driven Care and Services

Performance Standards:

A. There is consumer representation throughout the organization and consumers play an influential role on the full range of policy related and decision making entities such as: Policies and procedures committees, key standing committees, task forces, workgroups, new staff interviewing and hiring panels, councils, and advisory and agency boards.

0 1 2 3 4 N/A

B. Consumers are employed in various positions within the organization that directly influence the provision of services. Consumers are hired to provide: Direct services such as leading and co-leading groups; advocacy such as participating in service planning at the request of the consumer; welcoming and orienting new consumers to the organization; and involvement in orientation and training of all new and existing staff in trauma-informed care and services.

0 1 2 3 4 N/A

C. The organization has a formal system in place to continuously gather consumer feedback, identify problem areas, and make improvements as needed. A high priority is placed on assessing consumers' perception of safety, choice, collaboration, trust, and empowerment through methods such as consumer advisory councils, consumer surveys and discharge interviews.

0 1 2 3 4 N/A

D. The consumer's voice and choice are respected and encouraged. Consumers' receive information about their rights and program opportunities, education about the impact of trauma, and exploration of options to ensure that they participate fully in making informed decisions about every aspect of their care. The program avoids direct or subtle coercion or punitive actions when consumer choices/preferences are inconsistent with program recommendations.

0 1 2 3 4 N/A

Comments on Domain 2: _____

3. Trauma-Informed, Educated and Responsive Workforce

Performance Standards:

A. The organization’s leadership communicates a clear and direct message that the organization is committed to creating a trauma-informed system of care and that every employee is critically important in accomplishing this mission. This message is communicated through all of the following: Job advertisements, orientation process, job descriptions, employee handbook, supervision, staff development, and the organization’s website.

0 1 2 3 4 N/A

B. The organization places a high emphasis on the active participation and buy-in of senior clinical leadership in all trauma-informed care efforts.

0 1 2 3 4 N/A

C. All staff (administrators/supervisors, practitioners, employed consumers, and support staff) in the organization are educated about what it means to be a trauma-informed care organization, why it’s important and how *every* person in the organization plays a role in creating a safe and trusting “*healing*” environment.

0 1 2 3 4 N/A

D. Hiring practices (advertisements for new staff, job descriptions, and consumer involvement in hiring decisions) indicate that candidates who have training and experience in trauma related interventions and services, are highly valued and preferred.

0 1 2 3 4 N/A

E. Job performance evaluations clearly describe staff expectations and behaviors that are aligned with trauma-informed care principles.

0 1 2 3 4 N/A

F. Supervisors and practitioners receive training in trauma specific evidence-based and emerging best practices on an ongoing basis. The organization ensures that supervisors and practitioners are supported in further developing their trauma-informed care competencies; including having access to tools and resources such as curriculum based materials and practice guidelines.

0 1 2 3 4 N/A

G. Support staff receives ongoing training, performance evaluations, and supervisory assistance in integrating trauma-informed care principles in their work. Supervisors clearly demonstrate and reinforce that all staff have a role in creating a trauma-informed care environment.

0 1 2 3 4 N/A

H. The organization recognizes that staff success and satisfaction with their work might be affected by their personal trauma histories, compassion fatigue, secondary trauma also known as vicarious trauma, and the lack of organizational supports. The organization creates an environment that is safe and comfortable for staff to share personal and work related stressors and receive support through supervision; an Employee Assistance Program (EAP) or other professional services; training to increase confidence and competence in one's job performance; and education to increase awareness about the impact of stress on work performance and develop personally meaningful and useful stress management strategies.

0 1 2 3 4 N/A

Comments on Domain 3: _____

4. Provision of Trauma-Informed, Evidence-Based and Emerging Best Practices

Performance Standards:

A. The organization emphasizes the role of traumatic life experiences as key contributing factors in the development of many mental health, substance use and physical health problems rather than placing an emphasis on personal deficits, weaknesses and disorders. This may be reflected in the degree to which exploration focuses on "What happened to you" rather than "What's wrong with you". Staff

training, clinical documentation, individual and group educational materials, informational materials (e.g. websites, brochures, surveys, newsletters) all reinforce this point.

0 1 2 3 4 N/A

- B. In accordance with the consumer's preferences, the organization's service planning process is designed to include key members of the consumer's support network, (e.g. relatives, caregivers, residential staff, probation officer) in order to support the consumer, their service plan and promote positive treatment outcomes. These partners in care receive education, information, resources, and guidance to increase their knowledge about the consumer's trauma related challenges and improve their ability to relate to and support the individual.

0 1 2 3 4 N/A

- C. Consumers are fully involved in decisions related to service planning; the selection of services and methods and review of progress and changes to their service plan including; medication changes and choice of practitioners and number and types of services. Service plans are designed to ensure that consumers identify their personal strengths, goals, and express agreement with their service plan.

0 1 2 3 4 N/A

- D. The organization routinely assists consumers to develop a wellness plan that is designed to prevent and manage a crisis. The crisis prevention part of the plan includes daily health promoting activities, identification of stressful triggers, early warning signs, and problem solving strategies. The crisis management part identifies who the consumer wants involved, preferred treatments and how the consumer wants the crisis to be managed. All staff directly involved in the consumer's treatment is informed about the consumer's wellness plan and how they can support it.

0 1 2 3 4 N/A

- E. The organization offers an array of trauma specific services; those that are recognized as evidence based, evidence informed and/or emerging best practices. The array of trauma specific services is sufficiently broad to meet consumer preferences and needs (e.g., preferences for gender or sexual orientation specific services).

0 1 2 3 4 N/A

- F. In accordance with the consumer's expressed preferences, the organization promotes collaboration, continuity and coordination of care with other service providers and organizations involved in supporting and treating the consumer (e.g. primary care, inpatient general/psychiatric hospitals, residential services). The organization engages consumers in making informed decisions regarding the kind of information shared, especially with respect to trauma related experiences, and how sharing this information with other providers will benefit the consumer. The organization provides trauma

related information that will assist other service providers to develop a service plan that will promote effective care and reduce the likelihood of re-traumatization.

0 1 2 3 4 N/A

Comments on Domain 4: _____

5. Create Safe and Secure Environments

Performance Standards:

A. The organization has a system in place to identify and implement policies, procedures, environmental conditions, activities, social climate, documentation and treatment practices that promote a safe and secure environment in order to avoid re-traumatization or re-victimization. The organization maintains a “safe and secure environment team” that includes representatives from leadership, practitioners, support staff, and consumers to continually assess and correct areas requiring improvement. Examples of environmental elements that may affect safety, security, comfort and respect include: signage, separate or reserved spaces, dress code, layout of group therapy rooms, pictures on walls and staff offices, lighting in the surrounding area at night, furniture, bathrooms and shared areas with other organizations/businesses.

0 1 2 3 4 N/A

B. The organization ensures that all administrators, staff and consumers recognize that they each contribute to creating a safe, secure, and recovery oriented environment. This may include the following: The establishment of safety promoting ground rules for groups that are developed and agreed to by consumers, community established agreements for the use of common areas, strategies to resolve conflicts and address aggression, prevention and promotion of alternatives to seclusion and restraints and expectations about how staff relate to one another and consumers, particularly with respect to coercion, power and control issues.

0 1 2 3 4 N/A

C. The organization has a system in place for consumers and staff to “safely” let the organization know when practices, interpersonal interactions and/or the environment are unsafe and inconsistent with trauma-informed care without fear of reprisal (e.g. consumer advisory council, quality assessment interviews, surveys, inquiries by staff as part of routine individual and/ or group meetings).

0 1 2 3 4 N/A

D. The organization has a system in place to review and follow up on incidences that involve threats, self-harm, altercations, invasion of privacy, harassment; those events that compromise a safe environment. This system supports consumers and staff directly and indirectly affected by the incident, offering opportunities in individual and/or group meetings to address concerns, answer questions, and learn about action taken to address the incident and reduce the potential for recurrence.

0 1 2 3 4 N/A

E. The organization ensures that staff is educated and trained in using trauma-informed care approaches to prevent and manage incidences that create serious emotional distress for both staff and consumers.

0 1 2 3 4 N/A

F. The organization recognizes that seclusion and restraint, including the premature use or overuse of medication to control a person’s behavior, is not treatment nor a problem limited to inpatient or residential settings and that the impact these practices have on consumers has profound consequences and can result in retraumatization and revictimization. The organization has a system in place to utilize alternative, non-coercive approaches; ones that promote empowerment, choice, and involvement of consumers through trauma-informed policies and procedures, staff training, and consumer education and involvement.

0 1 2 3 4 N/A

Comments on Domain 5: _____

6. Engage in Community Outreach and Partnership Building

Performance Standards:

A. The organization assumes a leadership role in engaging and educating community partners (e.g., courts, police, emergency services, primary care, hospitals, residences, mental health and substance use programs, the general public, etc.) about trauma-informed care. This may include organizing community workgroups, community wide educational conferences/forums, and town hall meetings that focus on promoting awareness of trauma prevalence, its impact on people’s lives, and the importance of providing trauma-informed care. The organization ensures involvement of consumers in the planning and implementation of these efforts.

0 1 2 3 4 N/A

B. The organization engages external partners in the care of individual consumers, with their permission and involvement, to promote and ensure system wide trauma-informed care. These external partners such as primary care facilities, substance use treatment programs, criminal justice system, residential programs and emergency departments are invited to participate in service planning and coordination of care meetings.

0 1 2 3 4 N/A

C. The organization engages in trauma-informed care awareness building through multiple messaging. The organization reaches out to family members, consumers, local organizations, and the general public through social media, websites, newsletters, posters, billboards, marketing, letters, and brochures to educate and inform them about the prevalence and impact of trauma and how to promote healing, recovery and resiliency.

0 1 2 3 4 N/A

Comments on Domain 6: _____

7. Ongoing Performance Improvement and Evaluation

Performance Standards

- A. The organization has a system in place to regularly measure performance on each of the core trauma-informed care domains. Data related to each domain is tracked, analyzed and used to address challenges and/or reinforce progress.

0 1 2 3 4 N/A

- B. The organization has the personnel and system in place to analyze trauma-informed care performance data and share outcomes with leadership, agency board, staff and consumers in a manner that is clear and easy to understand (e.g., simple graphs that illustrate whether the program is staying level, improving or declining in a particular domain).

0 1 2 3 4 N/A

- C. The organization has a standing work group of key stakeholders empowered to sustain a continuous organizational focus on trauma-informed care. The group includes high level leadership with authority to address barriers, secure resources and influence the commitment of the workforce to uphold the principles and goals of trauma-informed care. This team utilizes the data and develops action plans that contribute to positive performance outcomes.

0 1 2 3 4 N/A

Comments on Domain 7: _____

Trauma Informed Assessments: Resource Guide

What is Trauma: “Individual trauma results from an event, series of events, or set of circumstances that is experienced by an individual as physically or emotionally harmful or life threatening and that has lasting adverse effects on the individual’s functioning and mental, physical, social, emotional, or spiritual well-being.” (SAMHSA, 2014)

What is Trauma Informed Care or a Trauma Informed Approach: “realizes the widespread impact of trauma and understands potential paths for recovery; recognizes the signs and symptoms of trauma in clients, families, staff, and others involved with the system; and responds by fully integrating knowledge about trauma into policies, procedures, and practices, and seeks to actively resist re-traumatization.” (SAMHSA, 2014)

How can I tell if my organization supports traumatized patient by providing a safe and supportive environment? Conduct a trauma informed assessment, and there are many:

Trauma Informed Assessments*

Title/Agency	Cost	Links
Trauma Informed Care Project Agency Self-Assessment	Toolkit is free, training is by request and costs \$	http://www.traumainformedcareproject.org/resources/Traum%20Informed%20Organizational%20Survey_9_13.pdf
Traumatic Stress Institute: ARTIC (Attitudes Related to Trauma Informed Care)	Pricing starts at \$750 for up to 500 respondents for the pencil and paper version, online version is also available	https://traumaticstressinstitute.org/the-artic-scale/
CCTIC: Creating Cultures of Trauma Informed Care	Protocol is publicly available, consulting is \$	https://children.wi.gov/Documents/CCTIC-Self-AssessmentandPlanningProtocol0709.pdf
National Council for Behavioral Health: Trauma Informed Care Training and Consulting	Cost: Customizable to organization, \$2500 per trainer, per day + travel	https://www.thenationalcouncil.org/wp-content/uploads/2016/12/TraumaInformed_1pager-FINAL.pdf?daf=375ateTbd56
ProQOL	Free, publically available-The ProQOL is the most commonly used measure of the negative and positive effects of helping others who experience suffering and trauma.	https://www.proqol.org/ProQol_Test.html
The Sanctuary Model: SELF toolkit	Not publically available, cost unknown	http://www.thesanctuaryinstitute.org/about-us/the-sanctuary-model/

Title/Agency	Cost	Links
CCSI Trauma Informed Care Organizational Self-Assessment (TIC-OSAT)	TRUST tool is free- trauma responsive understanding self-assessment available for organizations and TRUST-S available for schools	https://www.ccsi.org/Pages/TRUST https://trust-survey.com/FAQs
Thrive initiative: Trauma Informed Agency Assessment	Specifically for organizations that work with children	https://nhchc.org/wp-content/uploads/2019/08/thrive-guide-to-trauma-informed-organizational-development.pdf
Trauma Informed System Change Instrument	Free, focus on child welfare	https://traumainformedoregon.org/wp-content/uploads/2014/10/Trauma-Informed-System-Change-Instrument-Organizational-Change-Self-Evaluation.pdf
TReSIA: Trauma Responsive Systems Implementation Advisor	Free, offers paid courses via The trauma informed academy	https://epowerandassociates.com/epa_pdf_files/Sec_03-TReSIA-Assessment.pdf https://thetraumainformedacademy.thinkific.com/
TRST: Trauma System Readiness Tool	Free	https://surveygizmolibrary.s3.amazonaws.com/library/113599/TraumaSystemReadinessToolMarch2017electronic.pdf

*Assessment tool summary is adapted from The Greater Richmond Trauma Informed Community Network.

<https://www.acesconnection.com/fileSendAction/fcType/0/fcOid/472643003945852857/filePointer/472643003945852886/fodoid/472783741443508700/GRTICN%20Trauma-Informed%20Organizational%20Assessments.pdf>

Trauma-Informed Care in Youth Serving Settings: Organizational Self Assessment **

Directions: Please rate the items listed in the various categories. Please write comments about why you rated items in a particular way on the back side of each page.

This list is meant to be comprehensive and the process of implementing trauma-informed care generally takes multiple years. While implementation of these elements is the goal, the list represents an ideal to strive for.

	How much is this value embraced by your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very Much
Trauma-Informed Care Values	
<p>The following values underlie all the elements of trauma-informed care listed below. These values underlie the relationships between staff and clients, staff and their peers, as well as supervisory staff and their supervisees. Inherent in these values is the belief that all aspects of the organization's functions should be shaped by consumer involvement and input.</p>	
1. Safety – physical and emotional safety.	1 2 3 4 5
2. Trustworthiness – creation of a feeling of trust and safety via clear and thoughtfully considered frame and boundaries governing all aspects of the organization's work.	1 2 3 4 5
3. Collaboration – inviting, whenever possible, the input of those served by the organization and staff of the organization; providing opportunities for decision-making and innovation.	1 2 3 4 5
4. Empowerment -- sharing power with, and giving appropriate authority and decision-making power to, those served by the organization and staff of the organization; maximizing choice and control for the organization's consumers and employees; recognizing and highlighting strengths; looking for opportunities to praise and reward positive behavior; viewing mistakes as learning opportunities.	1 2 3 4 5

**** Significant sections of this assessment were adapted from the work of Fallot, R.D. & Harris, M. (2006). *Trauma-informed services: A self-assessment and planning protocol, version 1.4*. Community Connections: Washington, D.C. (202-608-4796).**

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very much
A. Administrative Support for Program-Wide Trauma-Informed Services	
1. Organizational administrators support the integration of knowledge about violence and abuse into all program practices.	1 2 3 4 5
2. The organization has a “trauma-informed care initiative” (e.g., workgroup/task force, trauma specialist) endorsed by and authorized by chief administrator.	1 2 3 4 5
3. A competent person with administrative skills and organizational credibility is designated to lead this task force.	1 2 3 4 5
4. Administration supports the recommendations of the trauma task force and follows through on these plans.	1 2 3 4 5
5. Administration attends at least portion of trauma training themselves (vs. sending designees in their places); they allocate some of their own time to trauma-focused work (e.g., meeting with trauma initiative representatives, keeping abreast of trauma initiatives in similar program areas).	1 2 3 4 5
6. The administration release staff from their usual duties so that they may attend trainings and deliver trauma services.	1 2 3 4 5
7. Necessary sources of funding for trauma training and education are found.	1 2 3 4 5
8. The administration is able to tolerate certain level of organizationsl disruption in making the transition, including such things as staff confusion, conflict within treatment team, resistance to change, and property destruction.	1 2 3 4 5
9. The administration values and rewards staff efforts to be flexible and to offer choices to the clients, even when the result is that the client is not immediately brought under control.	1 2 3 4 5
10. The administration develops a policy statement that refers to the importance of trauma and the need to acknowledge consumer experiences of trauma in service delivery.	1 2 3 4 5
11. The administration celebrates successes.	1 2 3 4 5

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very
B. Organizational Structure	
1. Clinically-trained staff are in leadership positions of multi-disciplinary treatment teams and are integrated into the daily life of programs.	1 2 3 4 5
2. In congregate care, organization has an organizational and supervisory structure where clinical and residential staff are integrated into treatment teams rather than belong to separate clinical and residential “silos.”	1 2 3 4 5
3. Intake and discharge process are planful, recognizing the important meaning of relationship beginnings and endings for traumatized children.	1 2 3 4 5
4. Staff schedules are structured such that staff have time to meet, think about, and talk about the work rather than only doing the work.	1 2 3 4 5
5. Staff have regular clinically-oriented supervision, ideally individual supervision, where they can discuss client issues including their countertransference and vicarious traumatization.	1 2 3 4 5
6. Forums (ie. supervision, treatment team meetings, periodic retreats) aimed at helping staff to acknowledge, address, and transform their vicarious traumatization.	1 2 3 4 5
7. Organization makes use of outside consultants who have expertise in trauma when necessary.	1 2 3 4 5
C. Trauma Screening and Assessment	
1. The program has a consistent way to identify individuals who have been exposed to trauma and to include trauma-related information in planning services with the client.	1 2 3 4 5
2. Trauma screening is relatively brief, not overly complicated, and avoids unnecessary detail that would increase likelihood of triggering traumatic memories.	1 2 3 4 5
3. The screening process avoids unnecessary repetition of same questions at multiple points in the intake or assessment process. It is often important to return to the questions in treatment after some appropriate time interval.	1 2 3 4 5

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very
D. Milieu Treatment Practices and Behavior Management (for congregate care settings)	
1. Staff and clinicians routinely think first about the meaning and function of behaviors before deciding how to intervene.	1 2 3 4 5
2. Staff display an attitude of the child “doing the best that they can” rather than assuming intentionality.	1 2 3 4 5
3. Staff use active listening to explore the problem rather than immediately speaking to the child about consequences or solving the problem.	1 2 3 4 5
4. Staff refrain from power struggles with children.	1 2 3 4 5
5. Organization uses of relationship-based behavior management system (such as The Restorative Approach™ *) instead of “point and level” system. Phase system can be used.	1 2 3 4 5
6. During behavioral issues, staff recognize primary goal as helping children to calm down and get back in control of their behavior.	1 2 3 4 5
7. Staff are sensitive to the many ways their interactions with children can trigger shame.	1 2 3 4 5
8. Staff refer to children in descriptive ways and refrain from negative labels (e.g. “manipulative,” “resistant,” “borderline,” etc.)	1 2 3 4 5
9. Staff value flexibility and individualized care in managing behavior rather than strict compliance with rules and treating all children equally.	1 2 3 4 5
10. Multidisciplinary team members function well as a team - manage conflict, care for each other, avoid splits such as therapist/child care worker splits.	1 2 3 4 5
11. Program has thoughtful physical touch policy that recognizes the critical importance of touch for healthy child development and is sensitive to issues of child abuse, allegations of abuse, and re-traumatization.	1 2 3 4 5
12. Staff are willing to talk with their peers and supervisors about their strong positive and negative reactions to clients and doing the work.	1 2 3 4 5
13. Staff feel free to ask their peers for help, or take over for a peer, when there is an impasse in managing a behavioral issue.	1 2 3 4 5

* The Restorative Approach™ is a trauma-informed behavior management system and an alternative to a “point and level system.” For information, contact Klingberg Family Centers, 860-832-5507.

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very
E. Physical Environment and Layout of Agency	
1. Space, including waiting and reception area, is welcoming and inviting for clients and families.	1 2 3 4 5
2. Living or program space is nurturing (e.g. colors, plants, music) and affirming (e.g. display of child art/work, culturally competent).	1 2 3 4 5
3. Crisis or “calm down” rooms are safe and soothing places for children to get strong feelings under control.	1 2 3 4 5
F. Clinical Treatment Practices	
1. Utilization of crisis prevention plans (also called safety tools or personal safety plans) written in collaboration with child, family, and possibly previous providers.	1 2 3 4 5
2. Before addressing problem behavior, the team, led by the clinician, considers their understanding of the reasons for the behavior and uses this understanding to determine their interventions.	1 2 3 4 5
3. Treatment planning is built from formulation that considers impact of trauma on client’s development and current symptoms/behaviors, and includes goals of developing emotion regulation skills/self capacities as well as healthy attachments.	1 2 3 4 5
4. Family therapy addresses family dynamics, builds parenting skills, and reinforces child’s growth and changes.	1 2 3 4 5
5. Staff have an awareness of the role of trauma in the history of parents, and family treatment includes a trauma focus.	1 2 3 4 5
6. Discharge is careful, thoughtful, gradual and includes referral to trauma-informed resources.	1 2 3 4 5
7. Program offers trauma-specific treatments such as: Trauma Focused Cognitive Behavior Therapy (TF-CBT), Dialectical Behavior Therapy (DBT), Eye Movement Desensitization Reprocessing (EMDR), Trauma, Adaptive, Recovery Group Education and Therapy (TARGET), etc.	1 2 3 4 5
8. Treatment utilizes sensory interventions to help children calm down and teach self-soothing.	1 2 3 4 5
9. Psycho-educational groups about trauma are offered to clients and families.	1 2 3 4 5

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very
G. Restraint and Seclusion Reduction	
1. All levels of staff are aware of propensity for re-traumatization through restraint and seclusion with traumatized clients.	1 2 3 4 5
2. Restraints and seclusion used only when there is threat of imminent danger.	1 2 3 4 5
3. Staff training focuses on de-escalation techniques to avoid restraint and seclusion.	1 2 3 4 5
4. Staff value avoidance of re-traumatization via restraint and seclusion even if it means less adherence to rules, increased property damage, and longer negotiation time.	1 2 3 4 5
5. Each child has an individual plan stating both medical and psychological risks in restraint which includes specific guidelines for staff actions to avoid.	1 2 3 4 5
6. Organization monitors trends in restraint and seclusion. Increased in restraint/seclusion trigger discussions aimed at understanding and addressing the increases.	1 2 3 4 5
H. Workforce Development	
1. Trauma training is required for staff at all levels and of all disciplines (see “Staff Trauma Training” below).	1 2 3 4 5
2. Staff who display mastery of trauma-informed practice are encouraged, celebrated, and promoted.	1 2 3 4 5
3. Organization promotes a culture of performance improvement, one that understands that mistakes will be made but learning will occur.	1 2 3 4 5
4. Trauma-informed values and concepts are integrated into staff orientation.	1 2 3 4 5
5. Hiring practices screen for staff whose values are consonant with a trauma-informed approach.	1 2 3 4 5

	How much is this element present in your organization?
	1=Not at all 2=Slightly 3=Moderately 4=Mostly 5=Very
I. Staff Trauma Training	
1. All staff members receive foundational trauma training with a primary goal of sensitization to trauma-related dynamics and the avoidance of re-traumatization.	1 2 3 4 5
2. Staff members receive training in a trauma-informed understanding of unusual or difficult behaviors. Training stresses concept of symptoms as adaptations.	1 2 3 4 5
3. Staff trauma training also includes topics of: frame and boundaries; relationship building with traumatized children; how to use their responses to particular clients (countertransference); impact of, and how to address, secondary trauma such as vicarious traumatization (VT).	1 2 3 4 5
J. Monitoring Trauma-Informed Initiatives	
1. Organization monitors the progress of trauma-informed care initiative in ongoing way.	1 2 3 4 5
2. Data related to implementation of a trauma-informed approach is collected, monitored, and used for quality improvement.	1 2 3 4 5
3. Organization develops a debriefing process to analyze incidents characterized by conflict, violence, and aggression to inform policy, procedures, and practices in order to avoid such incidents in the future.	1 2 3 4 5

Sources:

Harris, M. & Fallot, R.D. (Eds.) (2001). *Using Trauma Theory to Design Service Systems*. New Directions for Mental Health Services, Volume 89. San Francisco: Jossey-Bass.

Lang, J.M. & Franks, R. (2008). Connecticut TF-CBT Learning Collaborative Change Package. Adapted from Markiewicz, Amaya-Jackson, L., Agosti, J., & Lang, J. (2007). TF-CBT Organizational Assessment. National Center for Child Traumatic Stress.

Massachusetts Department of Mental Health (2008). *Resource guide: Creating positive cultures of care, second edition*. Massachusetts Department of Mental Health, Child and Adolescent Division: Boston, MA (617-626-8090).

National Association of State Mental Health Program Directors (NASMHPD) (2006). *Creating trauma informed systems of care for human services setting: Curriculum*. Alexandria, VA. www.nasmhpd.org.

Saakvitne, K.W., Pearlman, L.A., Gamble, S., & Lev, B.T. (2000) *Risking connection: A training curriculum for working with survivors of childhood abuse*. Sidran Press: Baltimore, Maryland.

#	Name	Developer	Description	Target Audience	Survey Completed By	Link and Permissions	Total # of questions	Cost	Psychometric Properties	if used or adapted for populations we are interested in	Comments	Further information
1	Trauma-Informed Agency Assessment (TIAA)	Maine Dept. of Health and Human Services	Measures core elements of TI Practice, Areas of service delivery, from the perspectives of the participant. 5 point likert scale with 25 items to assess whether agencies serving children who experience trauma and their families are TI. More information at http://www.maine.gov/dhhs/OI/PDF/Florida_Conference-SKG-handout.pdf . The TIAA measures the following domains of TI Practices: • Physical and Emotional	Child, Youth, & Family Serving Agencies, Residential facilities	For family members receiving services directly or who are caregivers of a young person receiving services.	http://www.t2bayarea.org/resource/erid/tia_thrive.pdf	25	Free. Permission needed for use Developer requests data collection Contact: Jay.Yoe@maine.gov	Results from data collected during the first statewide implementation for each of the six domains ranged between 0.80 and 0.93. This suggests	No adaptation needed if parent/family member is the respondent. Need to contact the author for scoring.	Used statewide in Maine Maine's Children's Behavioral Health Services. Only appropriate for clients of child and family service agencies. Does not assess at TI policies directly.	Steps to becoming a TI org is at http://thriveinitiative.org/thrivetraining/wp-content/plugins/ras-GroupManager/rgm_uploads/THRIVE%2
2	Trauma-Informed Program Self-Assessment Planning Protocol	Roger D. Fallot, Ph.D. & Maxine Harris, Ph.D.	Organizational readiness assessment protocol conducted by external trauma consultants to help agencies create an action plans/educational plans. A discussion format followed by questions and prompts. Questions address both services-level and admin or systems-level changes. The six domains assessed are: program procedures and settings; formal services policies; trauma screening, assessment, service planning and trauma-specific services; admin support; staff trauma training and education; and human resources	Child/Adult Serving Agencies/Programs	Full staff and patients interviewed with open-ended questions (probes)	The self-assessment planning protocol is at https://www.healthcare.uiowa.edu/icmh/documents/CCTICSelf-AssessmentandPlanningProtocol0709.pdf , and the self-assessment is at http://www.theanninstitute.org/TIP/SASCORESHEET.pdf	44	Free.	Not available.	It has been adapted to an interview format. Easier for implementation. See http://mha.ohio.gov/Portals/0/assets/Initiatives/TIC/CCTIC%20Program%20Finality%20Scale%20v1%203%201-14.pdf	This is the original tool that most tools are based on. Good tool to assess implementation of TI in organizations and to facilitate TI modifications in organization's service systems. Very detailed and comprehensive. Considerable	
3	Organizational Self-Assessment: Adoption of Trauma-Informed Care Practice	National Council For Community Behavioral Healthcare	It is designed primarily as a performance improvement resource to increase an organization's awareness of the key components of a traumainformed care organization. Consists of six TIC domains of TI policies and procedures: Early screening and assessment of trauma; consumer driven care and services; TI educated and responsive workforce; provision of TI practices; create safe and secure environments; engage in community outreach and partnership building. A seventh domain was added to assist an organization in assessing its readiness to measure and evaluate performance improvement.	Behavioral Health or other Child/Adult Serving Agencies/Programs interesting in screening, assessment and treatment of trauma	Can be independently completed by a range of stakeholders including; leadership, supervisors, practitioners, consumers, and support staff.	http://www.nationalcouncildocs.net/wp-content/uploads/2014/01/OASA-FINAL_2.pdf	34	Free. Use of tool is part of a larger consultation package with the National Council Contact: cheryls@thenationalcouncil.org.	Not available.	See a webinar for more info: http://www.thenationalcouncil.org/wp-content/uploads/2012/11/Is-Your-Organization-Trauma-Informed.pdf	Each question is lengthy and needs to be interpreted before selecting a response. More appropriate for upper level management.	
4	Trauma-Informed Care Organizational Self-Assessment for Consumer-Run Organizations	Wisconsin Dept. of Health Services	This tool is an adaptation from the TI Toolkit from National Center on Family Homelessness. Has 67 questions assessing TI practice (not screening and EBP trauma treatment) 13 questions to assess which training topics were received. 12 organizational assessment questions to assess supervision and practice protocols 10 questions assessing physical environment 4 questions on consumer rights 4 question on cultural competence 6 on privacy 9 on safety and crisis prevention planning 4 on openness and respectful communication 5 on consistency and predictability	Consumer-Run Recovery Organizations Child/Adult Serving Agencies/Programs providing services in a trauma-informed way	Questions are for supervisory and direct service staff	http://mha.ohio.gov/LinkClick.aspx?linkid=lsmxPQH0DUao%3D&portalid=0	67	Free	Not available.		The tool is appropriate for assessing training related to awareness/knowledge of the staff in addition to TI policies and practices. Does not assess leadership commitment. Note: this was adapted # 8 and is similar to #6.	
5	Creating Trauma-Informed Care Environments: An Organizational Self-Assessment	University of South Florida	For organizations just beginning or already practicing principles of Trauma-Informed care. Assesses 3 domains: (1) organizational readiness for trauma-informed care change; (2) competent trauma-informed organizational, clinical, and milieu practices; and (3) consumer and family engagement. More information at http://www.dcf.state.fl.us/programs/samh/mentalhealth/training/ba/Trauma%20Web%20Event/Informed/Trauma_Informed_care.p	Child/Adult Serving Agencies/Programs. Can be used for residential youth settings.	Questions are for supervisory and direct service staff and those in leadership role	http://www.cfhn.org/assets/TIC/you	25	Free	Not available.		Shorter tool. But the wording seems to be geared towards a higher reading level.	
6	Trauma-Organizational Self-Assessment	Orchard Place/Child Guidance Center's Trauma Informed Care Project	This tool is an adaptation from the TI Toolkit from National Center on Family Homelessness. Has 62 questions assessing TI practice AND 38 on TI screening and adapting to TI policies : 29 questions on Supporting Staff development 33 on Creating a safe and supportive environment (consumer rights, cultural competence, privacy, safety and crisis prevention planning, openness and respectful communication, consistency and predictability) 26 on Conducting Intake Assessments	Child/Adult Serving Agencies/Programs	Administrative and supervisory Staff – self-administered and scored by the organization	http://www.t2bayarea.org/resource/erid/tia_orchard.pdf	97	Free	Not available.		Comprehensive and well-suited for most sites. Note: this was adapted # 8 and is similar to #4.	
7	TreSIA Self-Assessment	epower & associates	The first section is the self-assessment about how TI the organization is. 50 items on a 5-point likert scale. The second section helps interpret the scores and to assess where the organization is relative to key characteristics in environments that operate from a trauma-informed perspective. Five areas: leadership and culture; TI care/responsive structure; policies and processes; employee skills; tools and resources.	Mental health and social service Agencies/Programs.	Self-administered staff survey intended as a team based activity to support the development of a change plan. Protocol provides recommendations for actions based on scoring	http://www.traumainformedcare.com/TIC_PDF/Sec_03-TreSIA-Assessment.pdf	50	Free	Not available.	Questions need to be adapted to the programs being implemented at the Mental Health and social service agencies.	Questions seem to be very specific to the programs implemented. Please see sections 1 and 2 for information on Trauma-Responsive systems and Trauma-Informed Care at: http://www.traumainformedcare.com/TIC_PDF/Sec_01-TreSIA-Intro.pdf , and http://www.traumainformedca	

8	Trauma Informed Organizational Assessment	National Center on Family Homelessness	123 questions on TI practice with screening and referral tailored to homeless 2 items added for physical environment 2 more items for information sharing; 1 on cultural competence and 4 more on privacy 18 more items on practice skills 7 more on involving consumers 1 more on policies	Developed for Homeless services. Could be used for any organization that provides treatment services.	Self-administered survey for all staff	http://www.pcamn.org/wp-content/uploads/2014/04/Trauma-Informed_Organizational_Toolkit_Homelessness-Services.pdf	135	Free	Not available.	Takes approx. 40 minutes to complete	Same tool #6, added questions on involving current and former customers. Has some specific questions on homelessness. Very long.
9	Trauma-Informed Organizational Self-Assessment for Child Abuse Prevention Agencies	Wisconsin Children's Trust Fund	101 questions on TI practice including screening and referral. Tailored to children 14 items on training and education 11 on staff supervision 8 items on physical environment 16 items for information sharing, cultural competence and privacy 45 items on practice 6 items on consumer involvement 9 items on policy	Child Abuse Prevention Agencies	All staff – self administered survey	https://www.dhs.wisconsin.gov/ti/s/acap.pdf	109	Free	Not available.		Same tool as #4, 6 and 8 See #6 for comments
10	Trauma Informed Care (TIC) Organizational Self Assessment	Shift Your Perspective Trauma Informed Care	Similar to #5, with minor wording modifications. Response options are the same as well. Tool # 5 has a couple of extra questions, minor change in wording, replaced "agency" with "organization". Response options are the same as well.	Child/Adult Serving Agencies/Programs	Fidelity items intended to be used as a part of an assessment that includes: Staff interviews Consumer interviews Policy/procedure review Chart review	http://www.t2bayarea.org/resource/brid/tia_shift.pdf	25	Free	Not available.	Might needed to be adapted to make it more specific to the organization.	Same Tool as #5. But this tool can accommodate other sources of information such as consumer record review. Not detailed enough compared to #2, 4, 6 and 8
11	Trauma Informed System Change Instrument	Southwest Michigan Children's Trauma Assessment Center's (CTAC)	Has 6 questions on policies and and 13 on practices. For the version to be completed by an individual, it has 3 on Integration and 3 on Openness	Individual practitioners and organizations Child/Adult Serving Agencies/Programs	Staff at all levels; peer providers, and volunteers	http://traumainformedoregon.org/wp-content/uploads/2014/10/Trauma-Informed-System-Change-Instrument-Scoring-Guide-and-Psychometrics.pdf	19	Free	Internal consistency ranges from .735 to .875. Factor loadings range from .57 to .85	The questions might need to be contextualized to the organization	Geared towards organizational and individual level. http://www.wmich.edu/sites/default/files/attachments/u248/2013/2012%20Factorial%20Validity%20of%20TISC1_0.pdf
12	TI Organizational Capacity Scale	American Institutes for Research	This 35-item measure the extent of which the org provides TI care agency-wide across five domains: 1) Build TI knowledge and skills, 2) Establish trusting relationships, 3) Respect services users, 4) Foster TI service delivery, 5) Promot TI procedures and policies. Items within each domain	Health and human service organizations (settings such as behavioral health, housing and homelessness etc.)	All staff – self administered survey online	http://www.air.org/sites/default/files/trauma-informed-care-instrument-one-pager-Feb-2016.pdf	35	Proprietary. Email Kathleen Guarino at kguarino@air.org	Psychometrically validated on a sample of 424 respondents representing 68 human service agencies. But psychometrics not available online.	unknown	The scale is good for measurement at single time point as well as to assess change in organizational TI policies and procedures.
13	Trauma Informed Practice (TIP) Scales	Sullivan and Goodman; National Center on Domestic Violence, Trauma, and Mental Health	33 items broken into 6 subscales: 9 items on environment of agency and mutual respect 5 items on access to information on trauma 3 items on opportunities for connections 3 items on emphasis on strengths 8 items on cultural responsiveness and inclusivity 5 items on support for parenting	Community programs/domestic violence	Completed by clients/DV survivors	https://vaw.msu.edu/wp-content/uploads/2015/02/Tips_Using_TIPS_Sullivan_Goodman_2015.pdf	33	Free	The validation study is available in the Journal of Community Psychology, Volume 44, Issue 6, Version of Record online: 11 JUL 2016		Good instrument for staff-level experience of TI practices. Questions are worded well.
14	Standards of Practice for TIC	Yatchmenoff, Diane from Portland State University	The standards are intended to provide benchmarks for planning and monitoring progress and a means to highlight accomplishments. Each section of the Standards references specific elements in the SAMHSA Guidance document.	Mental health, health, and human services organizations	Multi-level staff	http://traumainformedoregon.org/wp-content/uploads/2016/07/Guidelines-and-Standards-of-Practice-for-Trauma-Informed-Care-07-16.pdf	51	Free	Not available. Will email author	Questions need to be adapted if meant as self-report	Not a measure really but standards of TI practice. Not recommended for self-report, but more as focus groups or interviews.
16	Attitudes Related to Trauma-informed care (ARTIC)	Traumatic Stress Institute/Courtney Baker, Tulane	Three versions for each of the two settings (45 items, 35 items and 10 items). Longest version takes 15-20 minutes. Aims to determine if staff attitudes are favorable or unfavorable of TIC. Psychometrics available	Human Services; education	Completed by professionals and paraprofessionals	http://traumaticstressinstitute.org/artic-scale/	varies	Propriety - \$450 per organization. http://traumaticstressinstitute.org/how-do-i-obtain-the-artic/			

17	TICOMETER	Trauma institute	35 items across 5 domains measures the level of TIC, identify gaps in implementation. Assessment takes 15 minutes. Meant to be completed at multiple time points. Domains are: Knowledge Trusting relationships Respect for service users Service delivery Policies and procedures	Human services; behavioral health; substance abuse, housing, child welfare, domestic violence, community health centers, hospitals	Staff at all levels; peer providers, and volunteers	http://us.think3.com/ticometer	35	Propriety. Requires a \$25/year subscription for unlimited access to the tool Online and scores sent back immediately but additional fees to have scores aggregated across users – results in 1-2 weeks	Pilot tested with 68 organizations and 667 providers			
----	-----------	------------------	---	--	---	---	----	---	--	--	--	--

Scenario Facts 1: The Petition Hearing

Magistrate Lobato is presiding over a petition for a final civil protection order in a case involving domestic violence. The case is on the public docket and the courtroom has court staff, attorneys, advocates, and members of the public moving in and out of the chambers. The Respondent is representing himself and while cross-examining the Petitioner, begins yelling at the Petitioner and is becoming increasingly agitated. Magistrate Lobato does not have a bailiff in the courtroom and asks the clerk to contact the Sheriff. Before the Sheriff can arrive, the Respondent approaches the Petitioner and physically assaults and starts to strangle her. The Respondent renders her unconscious, runs out of the courtroom, and flees the courthouse. Paramedics also arrive to treat the Petitioner, who is taken to the hospital while still unconscious, and anyone else in the courtroom.

Scenario Facts 2 – After the Petition Hearing

Present in the courtroom to support the Petitioner during the assault is Rose, the Petitioner’s advocate, as well as the Petitioner’s attorney, Janice, who works pro bono for the local domestic violence shelter. Jeff, a new judicial employee and a recently discharged veteran was also present as he was training with the court clerk. The courthouse offices include a self-help center and multiple staff at the center worked with the Petitioner and Rose, helping them through the process of for applying for the protection order and connecting Petitioner with local domestic violence services, including the shelter and treatment.

Scenario Facts 3: The Community

The district where Magistrate Lobato presides covers four rural counties, and each county seat has a small courthouse, three of which were built over 30 years ago. The four counties include some small towns as well as small and more spread-out agricultural communities. Court funding in the district provides limited courthouse security measures, to include just a wand and metal detector bought from the federal government. In one county, the population is so small that a circuit judge only comes by once every two weeks to hear cases and there has never been security because people know each other. The Sheriff's Department provides additional security as well as response to any courthouse incidents within the various district courthouses. There is also a tribe in the district whose lands cover two states. The Petitioner is a member of one of the tribes located near the courthouse and the Respondent is not. The population in the district includes many migrant families that come in for seasonal work. Given the small population, many within the community have friends or family members that work in or around the courthouse.

DV AWARE
Collaboration Multiplier

Goal: Identify Partners for Successful Collaboration on Recovery & Engagement

Sectors/Partners*	Expertise*	Assets/Strengths*	Roles/Resources*	Key Strategies*

*Sectors/Partners: refer to those key stakeholders needed for Recovery and Engagement planning and implementation, including but not limited to government agencies, community organizations, culturally-specific organizations, victim-centered organizations, faith-based organizations, etc.

*Expertise: What unique expertise does this field bring to the collaborative?

*Assets/Strengths: What resources (skills, staff, training capacity, funding) can be brought to the table?

*Roles/Resources: What role will the partner play and what resources can they bring to the collaborative?

*Key Strategies: What key strategies/activities are currently implemented relevant to this issue?

Action Planning Worksheet

Space is available in the worksheet for individuals to identify their goals for improvement of their court/community's preparedness regarding domestic violence-related incidents.

MEANINGFUL & ONGOING COLLABORATION: WHAT ARE THREE STRATEGIES FOR IMPROVING YOUR COURT/COMMUNITY'S COLLABORATION ON SAFETY?

TRAINING AND EDUCATION: WHAT ARE THREE STRATEGIES FOR IMPROVING YOUR COURT/COMMUNITY'S TRAINING AND EDUCATION ON SAFETY?

EFFECTIVE PRACTICE: WHAT ARE THREE STRATEGIES TO IMPROVE YOUR COURT/COMMUNITY'S CURRENT SAFETY PRACTICES?

ADDITIONAL AREAS FOR IMPROVEMENT: WHAT ARE SOME OTHER IDEAS YOU HAVE/CAN COMMIT TO?
