

Court Security Resource Guide

A practical guide to the practices, procedures and resources available for those providing court security.



®



®

**National Sheriffs' Association
Court Officers' & Deputies' Association**

FOREWARD

For the majority of the nation, court facilities (“The Courthouse”) houses many, if not all of the functions of county government, notwithstanding court activities themselves. The Security of a courthouse is based on a balance between four essential components: involvement of all stakeholders, security personnel, technological devices, and the configuration of the facility itself. Absence of any one of these components affects the security of the facility. This guide is presented as an aid for those stakeholders who must bring about the balance

Security in the courtroom and the courthouse varies considerably through out the United States. In some states and commonwealths the Office of Sheriff is mandated to “attend court” while in some states no one is assigned the task. In a few instances responsibility for court security is divided or not clearly defined.

There have been limited structural or technological changes relative to facilities across the nation since the 1980s. Until recently, behavior of the local community, especially those attending court and conducting business in the courthouse did not warrant the use of additional security measures. The day of open and un-impeded access to the courts is quickly waning, as national trends continually reflect direct and deliberate violence toward the court system and those who work within the system every day.

In 1978 the National Sheriffs’ Association published the results of a two-year study relating to the security in the nation’s state and local courts. This study became a national reference for the improvement of court security. The National Sheriffs’ Association served as a consultant to the United States Marshals Service in the development and training of court security professionals. Intimidation, actual violence within the courthouse and courtrooms, outside assaults and abductions and increased juvenile and domestic violence have played out on or near our courts. Additionally, since September 2001 the new threat of terrorist attack by individuals merely wishing to inflict destruction on American soil and processes have been added to this mix of violence.

Events involving the courts and all its stakeholders clearly demonstrate the need to access the vulnerability of judges, staff, witnesses, and the general citizenry. Added to this equation is the increasing occurrence of violence within the workplace. Incidents involving employees, customers, and the relationship mix that is brought to the workplace has increased the need for a well-trained and informed staff. Security is no longer just protecting the court; it has expanded to a situation where courthouses and their immediate areas now need a security component that can only best be described as a police district in and of itself functioning as any unit with the duty to serve and protect.

ACKNOWLEDGMENTS

The following individuals have contributed to the input and design of this manual:

Barrett, Jimmie-Sergeant, Arlington Co. VA. CODA 2nd Vice President 2005

Beckley, Jo- Bailiff, Warren Co. KY. Past President IACOS (International Association of Court Officers and Services)

Burkhardt, Jim-Court Security Director, Clark Co. OH. CODA Board of Directors at Large.

Conrad, Greg-Major, Suffolk Co. NY. CODA 1st Vice President 2005

Coulter, David-Deputy Sheriff, Court Security Supervisor, Teton Co. WY. CODA President 2005

Gordanier, Robert-Chief Marshal, Aurora, CO., CODA Board of Directors West

Jackson, Michael-Sheriff, Prince Georges Co. MD., CODA Board of Directors East

Lorito, Tom-Former Chief, Suffolk Co. NY., Past President IACOS

Ludolph, Jim-Court Security Supervisor, Peoria Co. IL., CODA Board of Directors at Large

McCabe, Robert-Sheriff, Norfolk City, VA., CODA 3rd Vice President 2005

Robertson, Mike-Master Deputy, Greenville Co. SC., CODA Board of Directors East

Shader, Paul-Marshal Commander, Reno Municipal Courts, Reno, NV., CODA Board of Directors West

Smart, Philip-Marshal, Missouri Supreme Court, CODA Board of Directors West

Wade, Bill-Major (retired), Prince Georges Co. MD., CODA Board of Directors East

Zaruba, John-Sheriff, DuPage Co. IL., NSA Sergeant at Arms, NSA Board of Directors, NSA Court Security Committee Chairman, Founder and first acting President of IACOS, and author of this manual's introduction and Courthouse-Court Facility National Staffing Guidelines.

Chapter 1

INTRODUCTION

At one time, court security was usually considered only during high-risk or controversial trials. However, in the last few years, court security has become a daily concern of many law enforcement officers. Increased court violence has been brought to public attention by a few sensational court incidents, such as bombings, kidnappings, demonstrations and assaults – all part of increasingly violent behavior throughout society. However, most law enforcement officers in charge of court security recognize the need to prevent not only these isolated, usually spontaneous events, but also daily incidents that can hamper the administration of justice. Such incidents include emotional outbursts in the courtroom, destruction or theft of court records, and prisoner escape attempts.

In the absence of current research to determine actual levels of violence in and around courtrooms and courthouses, the National Sheriffs' Association is relying on previous research and current anecdotal material to proffer these guidelines and commentary. Further, this manual offers guidelines to help those in charge of court security plans for both daily problems and rare, sensational events. The guidelines and recommendations in this manual cannot be all inclusive. Instead, the suggestions here are meant to raise issues to be considered in current security plans and to offer possible ways to deal with those issues.

Violence in Civil Courts

Anecdotal evidence, past interviews and general practitioner commentary holds that over half of court incidents occurring today are in civil and domestic courts. The level of security awareness and the precautions taken in these courts are often less than in criminal courts, as parties to an action were not thought to be crime prone. However, there is an inescapable fact that in civil and family courts, someone usually loses their argument. Throughout the following chapters, civil courts are discussed in terms of the problems likely to occur and guidelines for improving security.

In interviews, NSA found intense security awareness after serious incidents, when the immediate response generally was: more security procedures, funding, and manpower. In many cases, these measures were either reduced or stopped completely after a few months, and the earlier levels of security resumed.

Use of Existing Security Measures

A major problem in some courthouses is that security procedures and equipment are often not adequate, maintained properly, or used effectively. For example, magnetometers (metal detectors) were understaffed, alarms were assumed to be false and thus not responded to, closed-circuit television is not monitored, and expensive equipment was inoperable because of poor maintenance. In many jurisdictions, security

can be greatly improved by reallocating personnel and/or strictly enforcing procedures already in effect.

Courthouse Construction

A serious problem during courthouse construction is the frequent lack of input from security personnel, often resulting in costly changes. This manual discusses that problem and suggests ways for a security planner to be involved in courthouse construction, renovation and remodeling.

Training

A well-trained staff able to anticipate and respond to different situations is one of the best deterrents to court incidents: thus, some formal court security training should be available for every law enforcement agency responsible for court security.

This manual discusses court security in terms of policy and procedures, physical security (including equipment and architecture), and personnel. Key issues in some of these areas are listed in the Appendix for easy reference, and many are discussed in more detail in later chapters.

Chapter 2 discusses: (1) the relationship of security to the criminal justice system, (2) threats to court processes, (3) measures taken to counter threats, and (4) responsibility for court security. Chapter 2 makes these major points and definitions:

“Court security” means the procedures, technology, and architectural features needed to ensure both the safety of people and property within the courthouse and nearby grounds and the integrity of the judicial process.

Security is needed daily, not just during special trials. However, it must not be so visible that it becomes repressive.

Effective court security helps preserve constitutional rights; although, court security staff also must consider legal guidelines and restrictions before carrying out security measures.

One person should be responsible for overall courthouse security.

Chapter 3, the most comprehensive part of the manual, gives the security planner information about developing policy and preparing two key publications – the security procedures and court officers’ manuals. These specific guidelines and recommendations are included in the chapter:

1. Prepare written court security policy statements.
2. Search the courtroom and related areas both before and after court convenes.
3. Provide adequate visitor control through directories, floor plans, receptionists, and special search operations, if necessary.

4. Prepare a contingency plan for hostage situations and special plans for high-risk trials. Also develop procedures for a fire, bomb threat, natural disaster, civil disorder, power or utility failure, or any other situation requiring a general building evacuation.
5. Provide for post event review of the response to any special situations.
6. Ensure security for judges, guard their parking spaces and assign parking by number rather than name, escort judges through public corridors, provide an alarm button in their chambers, and search chambers daily.
7. Provide private witness waiting areas if possible.
8. Provide court officers detailed written instructions for courtroom procedures and for handling juries both under normal circumstances and when sequestered.
9. Transport incustody defendants between jail and court by vehicle if a secure tunnel or bridge is not available.
10. Suggest additional security measures for the judge's approval when incustody defendants are expected to present a high security risk in the courtroom.
11. Recognize critical times when incidents may be expected – e.g., (1) at the appearance of an antagonistic witness or codefendant; (2) during prisoner movement between various points; (3) at arraignment and sentencing; (4) when commitment is ordered in juvenile court; (5) when a verdict is rendered in a domestic or small claims court; and (6) when unruly spectators are present.

The focus of chapter 4 is the physical security survey and how to conduct it. These are some of the recommendations made within the chapter:

1. The survey should include all building spaces, including both public and restricted or controlled areas, regardless of tenants.
2. A survey should be conducted by a team, rather than by just one person.
3. The survey team should meet with the department heads of tenant agencies before the survey to answer questions and ask for cooperation, and after the survey to review with them the draft findings, conclusions and recommendations.
4. Managers should draw up detailed plans to carry out all recommendations. Follow-up inspections are needed to find out if recommendations are being implemented.

Chapter 5 discusses equipment that may be needed in a court building and standards for choosing the right items, including ways to improve procurement procedures. These are some of the topics covered:

1. A suggested method to estimate and compare equipment and personnel costs;
2. Standards for selecting equipment, including need, suitability, performance, reliability, obsolescence, availability, design limitations,

- compatibility, cost, manpower impact, space needs, installation and maintenance;
- 3. Guidelines to prepare detailed equipment design or performance specifications;
- 4. Special provisions to include the invitation to bid (IFB).

Chapter 6 discusses personnel selection, assignment, use and training, specifically addressing:

- 1. Guidelines for developing job descriptions and standards for court security personnel selection and assignment;
- 2. Factors influencing training, such as available funds, resources and space; the number of people who can be taken away from their assignments temporarily; and state training requirements;
- 3. Steps a manager should take in developing a new training program, including selection standards for training officers.

Chapter 7 takes up architectural matters that will help security officers make recommendations to planners and become involved in the planning phase as early as possible. A few key recommendations follow:

- 1. Choose an architect with court design experience;
- 2. Set up separate entrances and circulation routes for incustody defendants, judges and court staff and the public;
- 3. Locate public offices on lower floors in multistory buildings, near public entrances and away from courtrooms to reduce noise and unnecessary traffic;
- 4. Carefully design the prisoner reception area. Ideally, it should be a sally port, or passageway, with the entrance not visible to the public and opening directly into a secure or restricted passage;
- 5. Improve courtroom security through design features or duress alarms for the judge, clerk or court officer to summon help; and
- 6. Design temporary holding areas to include provisions for separating prisoners, an observation port on the door of the holding room, privacy screens for toilet facilities and any other special features needed. One or more cells can be wired for sound and CCTV for use when an unruly defendant is removed from the court.

Security can be maintained in most court building by taking a few basic precautions. This manual is designed to make court security planners aware of the potential for disruption and solutions available to deal with the problem. Even if no incidents have occurred, every jurisdiction should carry out adequate planning.

Chapter 2

COURT SECURITY

This chapter describes court security in terms of the following:

1. The relationship of security to the criminal justice system;
2. Threats to court processes;
3. Measures taken to counter the threats; and
4. Responsibility for court security.

The chapter discusses general relationships between court security and the criminal justice system, as well as some legal restrictions and guidelines on certain security measures. The chapter analyzes threats in terms of types of incidents: who is the most likely to cause court violence; how trial participants view threats; and when and where threats are likely to occur. Measures taken to counter these threats include architecture, equipment and procedural innovations. Responsibility for court security is discussed in terms of key courthouse areas and the role and relationships of various court personnel.

The chapter gives background information on court security and sets the stage for the following chapters, which deal with these aspects of court security planning: procedural guidelines, physical security factors, equipment selection and purchase, personnel and training requirements and architectural considerations.

Background

Court Security Defined

Depending upon context, environment and purpose, “security” has many meanings. A sample of definitions follows:

- Security is an intangible quality, which can only be measured by its lack.¹
- Security is the absence of security failures in the face of security threats.²
- Security means preventing or detecting a dangerous incident and limiting the damage it causes.³
- Security provides either active or passive means to help protect and preserve an environment in which activities are not disrupted.⁴
- Security is a process of setting up barriers that combine to increase detection and apprehension, thus making criminal or violent acts too dangerous or costly.⁵

¹ F. Michael Wong, *Space Management and the Courts: Design Handbook* (Washington, D.C.: U.S. Department of Justice, 1973), p. 83.

² *Ibid.*, p. 84.

³ *Ibid.*

⁴ Richard S. Post and Arthur A. Kingsbury, *Security Administration: An Introduction* (Springfield, IL: Charles C. Thomas, 1970), p. 14.

In this manual, the term “court security” includes the procedures, technology and architectural features needed to ensure (1) the safety of people and property within the courthouse and nearby grounds and (2) the integrity of the judicial process. Thus, court security is an effort to prevent or control such problems as verbal abuse or insult, disorderly conduct, physical violence, demonstrations, theft, fire, bomb threats, sabotage, hostage situations, prisoner escapes, kidnappings, and assassination.

The key word here is “prevention.” Throughout this manual, court security is discussed in terms of what can be done to prevent incidents or hazards. Prevention involves procedures, adequate and sufficient equipment specifically to prevent theft and disorder within the courthouse. All policy and procedure should aim to reduce the opportunity for loss or threat of loss. At a minimum, policies and procedures should reduce the amount of any loss suffered.

Need for Court Security

The need for adequate court security is not a new phenomenon. Celebrated cases and notorious defendants did not begin recently. Court incidents in the United States go back at least to the trial of British soldiers after the Boston Massacre. However, modern court security is a relatively new activity, caused by a dramatic increase in court-related violence in the past few years.

Increased court violence has been brought to public attention by sensational court incidents. This violence has been a part of increasingly violent behavior throughout society – behavior often directed at social change. The courts, as highly visible symbols of authority and justice, have become logical targets and venues for expression and action. However, security is needed in daily operations as well as celebrated trials. Dramatic, widely publicized trials and violent acts have obscured the more numerous problems related to emotional outbursts, destruction or theft of court documents and records, prison escapes, fire, and general disruptions of the judicial process.

Security and the Criminal Justice System

Courts protect the freedom and property of all citizens by punishing those whom violate the law. Yet this process must preserve the civil liberties of all persons, for the alternative to a fair and effective legal system is either mob rule or tyranny. As Supreme Court Justice William Brennan wrote:

History has known the breakdown of lawful penal authority – the feud, the vendetta, and the terror of penalties meted out by mobs and roving bands of vigilantes. It has known, too, the perversion of that authority. In some societies, the penal arm of the state has reached individual men through secret denunciation followed by summary punishment. In others, the solemn power of condemnation has been confided to the caprice of

⁵ Allan Greenberg, *Courthouse Design: A Handbook for Judges and Court Administrators* (Chicago: American Bar Association Commission on Standards of Judicial Administration, 1975), p. 53.

tyrants. Down the corridors of history have echoed the cries of innocent men convicted by other irrational or arbitrary procedures.⁶

If the courts are to preserve constitutional rights, effective security is essential. Court disturbances threaten an orderly system of justice by interrupting the trial process and making it difficult for a defendant to obtain a fair trial. Disturbances also undermine public confidence in and respect for the legal process and may interfere with significant reform in the judicial system. In almost every way, disruption is inconsistent with the rule of law in a democratic society.⁷

Courtroom incidents have a profound impact on the administration of justice and, conversely, failings in the criminal justice system may stimulate disruptive behavior. Two Presidential Commissions have expressed shock at the lack of both fairness and efficiency in the lower criminal courts, particularly in urban centers. The President's Commission on Law Enforcement and Administration of Justice made the following comments in 1967, and they are also true today:

The commission . . . has seen cramped and noisy courtrooms, undignified and perfunctory procedures, and badly trained personnel. It has seen dedicated people who are frustrated by huge caseloads, by the lack of opportunity to examine cases carefully, and by the impossibility of devising constructive solutions to the problems of offenders. It has seen assembly-line justice.⁸

The following year, another national commission reported as follows:

The belief is pervasive among ghetto residents that lower courts in our urban communities dispense "assembly-line" justice; that from arrest to sentencing, the poor and uneducated are denied equal justice with the affluent; that procedures such as bail and fines have been perverted to perpetuate class inequities Too often the courts have operated to aggravate rather than relieve the tensions that ignite and fire disorders.⁹

The security measures needed to deal with disruptions and threats in courts should be viewed in terms of the negative influence they may have upon judicial proceedings. Security should be present, but not so visible that it becomes repressive. It is important to balance the safety of all trial participants against the need for fair and neutral proceedings.

⁶ *Illinois v. Allen*, 397 U.S. 337, 347-348 (1970).

⁷ Norman Dorsen and Leon Friedman, *Disorder in the Courts* (New York, New York: Pantheon, 1973), p. 17.

⁸ President's Commission on Law Enforcement and Administration of Justice, *The Challenge of Crime in a Free Society* (Washington, D.C.: Government Printing Office, 1967), p. 128.

⁹ *Report of the National Advisory Commission on Civil Disorders* (New York: Bantam, 1968), p. 337.

Legal Restrictions

Court rulings and state laws have set guidelines for court security measures allowed in certain circumstances. This discussion illustrates only a few of these guidelines, including methods to deal with unruly defendants and visitor control.

In 1970, the U.S. Supreme Court ruled that a judge has three alternatives for dealing with unruly defendants in the courtroom. The decision stated the following:

No one formula for maintaining the appropriate courtroom atmosphere will be best in all situations. We think there are at least three constitutionally permissible ways for a trial judge to handle an obstreperous defendant . . . (1) bind and gag him, thereby keeping him present; (2) cite him for contempt; (3) take him out of the courtroom until he promises to conduct himself properly.¹⁰

Many state laws and rules in the early 1970s were based on this ruling and dealt with different aspects of unruly court behavior. New York State amended its criminal procedure law to permit the trial of a defendant removed from the court for disorderly or disruptive conduct.¹¹ Nevada and Minnesota passed similar laws, and Massachusetts made disrupting court proceedings a criminal offense.

Legal precedent for searching all persons entering the courtroom and requiring them to register for identification purposes was set in 1934, when the Ohio Court of Appeals ruled that these measures did not amount to excluding the public. The court wrote as follows:

In the instant case it does not appear that the public was excluded from the courtroom; but every person who desired to enter the courthouse and pass the cordon of soldiers was required to have pass signed by either the judge or the Brigadier General in command of the militia, or both. It does not appear that any one was excluded who, after search and inquiry, was found to be a person of law-abiding intentions. We think the right to a public trial was not denied the defendant in this case.¹²

Many other court rulings deal with the security measures that can be used during trial proceedings. A few examples are listed here.

1. Additional guards may be ordered for courtroom security or to prevent disruption. *See People v. Burwell*, 44 Cal. 2d 18, 14 (1955); *People v. Santo*, 43 Cal. 2d 331 (1954); *People v. Stabler*, 202 Cal. App. 2d 862, 864 (1962); *People v. Harris*, 98 Cal. App. 2d 662 (1950).
2. Restraints may be ordered to prevent physical violence or disruption. *See People v. Kimball*, 5 Cal. 2d 609 (1936); *People v. Harrington*, 42 Cal.

¹⁰ *Illinois v. Allen*, 397 U.S. 337, 343-344 (1970).

¹¹ New York Crime Pro Law, 260.20, 3540.50 (McKinney 1972), chapter 789, 1971, laws of New York.

¹² *Pierpont v. State*, 195 N.E. 264, 267-268 (1934).

165 (1871); *People v. Burnett*, 251 Cal. App. 2d 651 (1967); California Penal Code, Section 688.

3. The court may order the defendant to be committed “at any time after his appearance for trial.” See California Penal Code, Section 1129; *People v. Cohen*, 1 Cal. App. 3d 94 (1969).
4. A court may control the use of its facilities during protests or demonstrations “to preserve the property under its control for the use to which it is lawfully dedicated.” See *Adderley v. Florida*, 385 U.S. 39, 47 (1966).

Absent any overriding justification, the constitutional rights of all persons having valid business with the Court should be permitted although this right often increases security risks.

Threats to Court Processes

Potential threats to court processes must be identified; then measures can be taken to reduce or eliminate those threats. This section identifies types of threats that may occur and then discusses the people likely to create them, how trial participants see threats and danger, and where threats are likely to take place.

Types of Threats or Incidents

Many types of threats are likely to involve courthouses and trial participants, such as:

- Escape or escape attempt;
- Disorderly conduct;
- Physical assault with a firearm;
- Physical assault with no weapon used;
- Bomb threat;
- Bomb explosion;
- Threat other than with bomb;
- Demonstration;
- Suicide or suicide attempt;
- Hostage situation;
- Physical assault with weapon other than firearm;
- Theft; and/or
- Fire.

Some examples of the specific threats or incidents which are disruptive to the judicial process are (from NSA studies and anecdotal commentary):

1. One criminal court defendant leaped to the bench and hit the judge on the head and shoulders with his shoe.

2. Another defendant kicked his court-appointed lawyer in the face and shoulders, knocking him to the floor.
3. A man involved in a civil lawsuit suddenly pulled out a gun and began shooting, killing a lawyer and wounding the judge and a witness.
4. A violent confrontation occurred between demonstrators protesting a trial and police outside a courthouse.
5. A fire in a court building destroyed several thousand court reporter tapes of trial testimony.
6. A judge was killed by a letter bomb sent through the mail.
7. A bomb exploded in the probation department of a courthouse.

This list illustrates the diversity of problems facing today's security planner.

Individuals Likely to Cause Threats

It is difficult to determine all risks in the court environment. Some risks are specific and communicated by words, actions or other notice. Other risks are more deceptive and require keen observation and action on the part of court officers. Risks can come from disturbed persons, political activists, persons who are protesting personal or court actions against them. Persons in all categories may play various roles in a trial, such as defendant, witness, and friend or relative of either the defendant or the victim. In addition, defendants and second, their friends or relatives often pose significant security risks. However, some incidents were caused by people with no known relationship to the judicial process.

A strong threat to court security occurs with very emotional defendants who are disturbed about charges facing them, sometimes unhappy with their lawyers, or concerned that the proceedings are somehow "stacked" against them. Factors that might contribute to their unruly behavior include revocation of bail, prosecution tactics, the judge's attitude, the presence of friends or relatives in court, and a long prison term or death sentence, loss of children, income, etc.

Ideas About Threats and Danger

Judges, lawyers, and court officers are often considered the trial participants most in danger. However, some court personnel believed that danger could only be determined by individual circumstances. For example, in a civil case the participant most in danger could be the winning litigant or attorney. During an armed escape attempt, the court officer or anyone in the way would be the main target, and in a hostage situation the judge would be the most likely victim.

Dangerous Areas

Threats can occur anywhere in or near the courthouse, which is divided into four areas in this discussion: the courtroom, nonpublic areas near the courtroom, public areas in the courthouse, and public areas outside the building.

The Courtroom Possible security problems in the courtroom include escapes or escape attempts, disruptions, and assaults. Escapes are a critical problem during trials, and attempts are especially likely at sentencing time. In highly publicized trials, or when defendants or their followers have a “cause” to make known, verbal disturbances may occur. Then too, defendants may try to assault trial participants because they are displeased with the trial or want to show disrespect for the proceedings.

In addition to these general threats, there are special security risks in the four courts discussed next.

Courts of First Appearance The courtroom where a person first appears for a hearing, arraignment, or other action is a very active area, and the large number of people in or near this courtroom often presents a security problem. Court officers, complainants, police officers, relatives and friends of defendants, attorneys, prison guards, spectators and defendants all may be in the courtroom at one time.

A common problem during arraignment is the defendant’s emotional state. Prisoners may wish to say goodbye to their families, turn over valuables for safekeeping, or give last minute instructions on personal matters. Yet defendants are being rushed into custody and must clear the bench area for the next case. Only rarely does a court have the facilities and personnel to handle these “last –chance” meetings. However, if those meetings are denied or cut short, the result may be a disturbance.¹³

Criminal Trial Courts Compared to an arraignment court, a criminal trial court is calmer, even for felony cases. However, there are certain security problems here, too. Well-known trials usually have a large number of spectators, and crowd control is a problem. Moreover, press coverage, defense and prosecution tactics, and background issues often heighten emotions. Finally, many courtrooms simply were not designed for trials with several defendants. Courtroom space becomes crowded when many attorneys and court officers are present, and security risks increase.

A particular type of criminal trial is the so-called “political” trial. Occasionally, the trial may have political overtones. Security problems during these trials may first arise when defendants try to complain about the indictments. If they believe the government is prosecuting for political purposes, they will complain publicly in the courtroom. Often, such defendants assume a defiant attitude throughout their trials, and such behavior usually attracts media attention. This gives the defendants an opportunity to convey a “political” message to a wide audience. The more disruptions, the more attention the trial will attract, and the more people will hear the message.

Civil Courts Functions common to the civil courts include appellate matters, probate, small claims, landlord and tenant actions, civil disputes between individuals and businesses, divorces, and claims against government agencies. In civil, as compared to criminal, matters, a major security difference is that people generally are not detained; therefore, guards, prisoners, and weapons usually are not in the courtroom. The greatest security threat during civil proceedings usually stems from the intense emotions that may be involved, as in divorce, child custody, eviction, and similar situations.

¹³ Wong, p. 85.

Juvenile Courts Juveniles in the court process present a special problem, mainly because of their unpredictable behavior. Thus, security officers must be constantly alert. Incidents in these courts may be irrational or involve a sudden angry outburst against parents or others, and an escape attempt may occur. These problems are discussed more fully in Chapter 3.

Nonpublic Areas near the Courtroom

These areas include judges' chambers, jury deliberation rooms, attorney-client conference rooms, witness waiting rooms, and temporary holding areas for incustody defendants. The primary security concern here should be to prevent easy access by the general public. Measures are needed to protect judges, isolate juries and witnesses from those whom may threaten them, and prevent escapes from attorney-client conference rooms and temporary holding areas, as well as assaults among hostile groups in the holding areas.

Public Areas in the Courthouse

Public areas in the courthouse are vulnerable to certain security problems, such as fire and demonstrations. Further, some areas (e.g., public restrooms, busy offices, hallways) may be used to hide explosives, and public hallways used as witness waiting areas outside courtrooms may be the scene of intimidation or assaults on witnesses.

Certain offices within the court building, such as the clerk of the court or the county treasurer, have unique security needs. The clerk's office is responsible for the safety and security of all court records, documents, case files, and, usually, trial exhibits. These items are vulnerable to fire, theft, and vandalism. Moreover, offices that collect fees, such as the clerk's office and the county treasurer, require special security precautions to prevent theft of the money.

Public Areas outside the Building

The security needs of public areas outside the court building should not be neglected. For example, the sidewalks and grounds of court buildings are possible sites of demonstrations, and threats or assaults may occur in parking areas.

Major Security Measures to Date

Traditionally, the courts take security measures only during certain high-risk trials. An example in 1933 involved the escape from an Ohio jail of John Dillinger, who was helped by three other men. During the escape, the sheriff was killed. The three accomplices were eventually caught and tried, and at the trial, the National Guard surrounded the courthouse, allowing entry only to individuals with a pass signed by the judge or the National Guard commander.¹⁴ All persons admitted to the courthouse were searched and required to register for identification purposes. Current high-risk trials have very similar provisions for visitor control.

¹⁴ See *Pierpont v. State*.

Yet, security has become a daily concern in many court operations and is now being considered in court building and renovation, equipment purchase, and general procedures. In designing courthouses and courtrooms, planners have included: key security features to protect judges; special corridors and holding areas for incustody defendants; and courtrooms with both the necessary decorum and security measures to protect all trial participants.

Close coordination should exist among judges, other court officials and security departments with the common goal for secure courts. However, the territorial and adversarial nature of justice often creates different dichotomies. In some cases, judges, sheriffs, and court administrators have formed security committees to consider actions to improve security. These committees focus on: defendants' rights; court decorum; security measures; and how appropriate those measures are to meet possible threats. In some cases, the committees even propose specific security ideas. In any event, the committees give security officers the chance to solicit the understanding and cooperation of judges in carrying out effective security plans.

Contingency planning has become the rule rather than the exception in recent court security operations. For example, high-risk trial plans include detailed procedures and identify who is responsible for each. There are special plans for bomb threats, plans to prevent weapons from being brought into court, judicial protection units, and plans for such events as natural disasters, medical emergencies, and building evacuations.

Many jurisdictions have found it necessary to develop mutual aid agreements with neighboring communities to meet equipment or manpower needs in certain emergencies. For example, most court security units do not have personnel skilled in bomb disposal, so they may seek help from a nearby sheriff's office, police department or a military installation.

A major change in recent years is the upgrading of court security personnel capabilities. In some cases, this has meant new performance requirements and selection standards for court assignment, including such factors as physical and psychological ability to handle violent persons, ability to cope with emergency situations, and knowledge of the security officer's role in the trial process.

Security Responsibilities

Responsibility for security in the courtroom and courthouse varies considerably throughout the country. In some cases, no one is specifically assigned either task, though some state laws assign the responsibility for one or both to the sheriff. In other jurisdictions, sheriffs have assumed responsibility because they are the most logical choice and the best prepared people available. In still other cases, court security seems to be the responsibility of everyone, with no clear authority given.

Even when overall responsibility is given to one person, others have authority for specific areas and operations. As a reminder, court security refers to the entire courthouse and its grounds. If responsibility is shared, coordination is needed between officials responsible for various types of security. However, the following analysis suggests that overall responsibility could effectively be given to a single official.

Courtroom

In the courtroom, responsibility should be clearly defined; indicating who provides security both during a trial and when court is not in session. During a trial, a deputy sheriff or court-appointed officer usually is present as a court officer to maintain order and deal with any violent incidents that occur. In addition, a deputy sheriff is usually responsible for the security of incustody defendants and for taking convicted defendants into custody.

When the court is not in session, responsibility for securing the room should be given to the department in charge of trial security. After hours, courtroom security may be provided by private guards if they are used for evening building security.

Nonpublic Areas near the Courtroom

Nonpublic areas near the courtroom include the judges' chambers, jury deliberation rooms, witness waiting rooms, and restricted passageways. The sheriff is usually responsible for security in these areas. However, the chambers may be a personal concern of the judge, whose interest must be reflected in security planning.

Public Areas in the Courthouse

Public areas in the courthouse include public hallways, restrooms, elevators, stairs and offices. Here security is sometimes given to the sheriff, whom incorporates procedures to protect public areas in an overall building security plan. Responsibility also may go to a county administrator, whom usually works closely with the sheriff.

Public hallways outside courtrooms present a special security problem. In many courthouses, witnesses wait there to be called, and their security should be assured.

Administrative offices such as the treasurer, clerk of the court, and assessor are often located in courthouses. Some of these offices are potential crime targets because money is collected there, while others are targets for people determined to disrupt the trial process. Often, too little attention is given to the security needs of these offices. County administrators usually are responsible for security, but, in some cases, they are uninformed about possible threats or the courses of action available.

After hours, the security of these areas must be maintained. Methods currently used include contracting with private guard services or making the sheriff, police department or county public works department responsible. Private guards may offer a cost-effective solution, but someone in charge of security should participate in preparing the work statement and help in contract negotiations. In addition, law enforcement should clear any guards chosen by the private company, if applicable, before they are assigned.

Public Areas outside the Building

These are areas next to the building, such as sidewalks, plazas, courtyards and parking areas. In many cases, municipal police departments handles security here. In case of a public demonstration, the police often will be able to provide the manpower and

equipment to contain the demonstration, while the court security staff will be concerned with preventing the demonstrators from entering the courthouse.

Recommendations

It is imperative that one person should be responsible for overall courthouse security. This person should show leadership in the provision of security for all the areas discussed here and should ensure the necessary coordination with other agencies, such as the local police department. As a professional security specialist, the sheriff is often the logical choice for this responsibility. Thus, the sheriff should have the right professional perspective, training and resources to prepare and execute sound security plans and make sure all requirements are met. Frequently, this responsibility is assigned by state law; otherwise, the presiding judge could make the assignment in a written order.

Court security means more than a modern building with the latest equipment. It means an understanding of the role court security plays in the criminal justice system, an evaluation of the threats to that system, and plans for an effective response to those threats.

Chapter 3

SECURITY PLANNING AND PROCEDURES

This chapter will give the security planner general information about developing a security planning effort as part of a systems approach, and will recommend subjects for both security procedures and court officers' manuals. These two manuals will provide clear, step-by-step instructions for court security personnel during both emergency and day-to-day operations.

Systems Approach to Court Security Planning

When starting or revising a court security program, it makes sense to use what planners call the "systems approach." This means taking several separate, but interrelated, parts and looking at the way they interact. In the security field, this kind of systematic analysis is easy – just follow the steps described in this section. First, however, some important terms will be defined.

Policies are general statements that guide people as they make decisions at various levels of an organization.¹ Policies are broad, comprehensive guidelines, while *procedures* are the specific methods to carry out those guidelines. The general goal of a comprehensive court security policy should be to establish appropriate protection for court staff and facilities, the general public, and the judicial process as a whole.

The planning process will result in specific procedures to carry out court security policy. Sheriffs or court-appointed officers responsible for court security must allocate limited resources to the areas with the greatest need. To do this successfully, they need to identify and rank security needs by a thorough assessment of threats and vulnerable areas in the courthouse.

The development of a security program can be broken down into five steps.²

1. Determine both short-term objectives and long-range goals.
2. List security problems to be remedied.
3. Consider possible solutions to those problems, including operational, technological and architectural remedies.
4. Test and analyze alternative solutions, then decide which one to try.
5. Prepare written policy and procedures statements.

Goals, Problems and Solutions

In order to address any situation, one of the first thing needed is a meeting of such key people as the sheriff, court security officer, presiding judge and court administrator. At this meeting, the program's overall goal and its objectives can be determined. For example, the goal may be to protect life, property, and the judicial process. The objectives may be to increase security for judges and jurors or to improve emergency

¹ H.S. Ursic and L.E. Pagano, *Security Management Systems* (Springfield, Ill.: Charles C. Thomas, 1974), p. 194.

² Richard S. Post and Arthur A. Kingsbury, *Security Administration: An Introduction*, 3rd ed. (Springfield, Ill.: Charles C. Thomas, 1977), p. 666.

response time. Any specific policies and procedures developed later must agree with those goals and objectives. This meeting will contribute to a positive security attitude among those running the court and will help gain cooperation with the security measures eventually adopted.

The second step is to identify and set priorities for the security problems within a building. This step should be started at the meeting and followed by a comprehensive survey of the courthouse, its occupants, and their duties.

An important aspect of the systems concept is choosing among alternative solutions to problems. In general, there are three types of solutions to court security problems: operational (through procedures and manpower); technological (such as installing an alarm system or using metal detectors); and architectural (new construction or renovation). The method ultimately chosen might involve only one category or it could be a combination of two or more.

Choosing the proper mix of manpower, materials, architecture, and procedures for a court facility is not always easy. For example, even in the most active court building, it is not necessary to make more than one courtroom suitable for high-risk trials because of limited demand and the high cost involved. One West Coast court spent more than \$700,000 to improve security for a single trial; obviously, most jurisdictions cannot afford such expenditures. However, significant improvements are possible through low-cost measures such as changing procedures, improving the quality of hardware, locking unnecessary doors, securing windows, and installing other devices that might be thought of after a comprehensive security study.

Many security measures overlap one another as good choices. For example, when judges and incustody defendants use the same restricted corridor, the result is a high security risk that can be prevented by somehow separating the two groups. An architectural solution to this problem would mean two separate corridors, while a procedural method would prevent prisoners from being in the corridor while it is used by a judge. The systems approach means looking at the limitations in each alternative before deciding on a plan. For instances, the architectural solution might not work because of the way the building is constructed, while the procedural method might require more manpower. The eventual choice also will depend on such factors as cost and judges' attitudes toward the idea.

The following general guidelines can help the security planner decide on the most appropriate solution(s):³

1. Space planning mainly deters or prevents dangerous situations, though this planning also helps court people detect security threats and can limit the damage from any incidents that occur.
2. Technology mainly helps court personnel detect security threats. The mere presence of technical equipment also can prevent incidents and help limit any damage.
3. Operational security measures, such as adding more security personnel, can deter and detect potential security problems, and can contain and control any situations that may occur.

³ F. Michael Wong, *Space Management and the Courts: Design Handbook* (Washington, D.C.: U.S. Department of Justice, 1973), p. 89.

Key Planning Factors

The security program is subject to both internal and external influences affecting both policies and the procedures to carry out those policies.

Community Pressures and Attitudes of Judges

The attitude of local citizens is important in many jurisdictions. A rural Midwestern sheriff explained the effect of public attitude on security measures this way:

In our community, where almost everyone knows one another by name, there is a limit on the restrictions that will be acceptable. The courthouse and courtroom have been traditional meeting places and always have been maintained in a fully accessible manner to all.

Situations like this require much skill on the part of the courts and law enforcement officials to “sell” legitimate and reasonable changes in the way courts are run. Another critical factor is the attitude of judges to security plans. Any plan, regardless of its merits, is useless if judges do not accept the idea. Thus, the security planner should work closely with the court and argue effectively for any new procedures which may meet resistance.

Legal and Budget Restrictions

Legal authorities should review draft security plans to make sure those plans comply with federal and state constitutions and statutes. A primary legal concern is to protect constitutionally guaranteed civil rights. In addition, safeguards also should be in place to protect the criminal justice providers from unnecessary harm or liability.

Next, a cost analysis is needed to determine which alternative security method is most economical. Cost enters a security analysis in several ways. First, how much money will a proposed security measure involve over the expected lifetime of the building? Second, how much do alternative measures cost? Finally, will expenses be offset by personnel reductions? All of these figures must be calculated for the expected lifetime of the building.

Getting more public funding for security might be difficult because the public cannot see the results as easily as they can when highways, schools, parks or other public facilities are built. When nothing visible or dramatic happens, security seems adequate, and legislative bodies traditionally are reluctant to spend funds on areas with little or no visibility.

Another major limitation, building design, is related to cost. When built 50 or more years ago, most court buildings lacked security features. Now many of these structures are unsuitable for remodeling or renovation to meet security needs, or the cost involved would be too great.

Program Implementation

To carry out the security program, written policy statements and procedures are necessary. A written policy is important because it (1) reduces the possibility of misinterpretation and error; (2) is a useful teaching tool;⁴ and (3) gives a framework for detailed procedures, thus providing a procedures checklist. Policy statements can be located for easy reference in both the procedures and court officers' manuals described later. For example, a manual section on handling incustody defendants should have an introductory policy statement followed by a set of instructions.

It is often necessary to obtain court orders to carry out the program in specific situations. The sheriff or security officer should keep a list of these and any other appropriate situations and should be sure that the necessary court orders are obtained, distributed to key personnel, and prominently posted for public examination.

Security Procedures Manual

The sheriff or court security officer should be responsible for maintaining the integrity of the court, the safety of building occupants, and the security of the building. To help achieve these objectives, all security personnel should have a security procedures manual that gives comprehensive, written instructions. Many jurisdictions, especially small ones, do not have such documents. Other areas have manuals that need updating. Although most court security departments have written instructions on certain aspects of its operation, such as handling bomb threats, few have comprehensive procedures for security throughout the courthouse. Therefore, each jurisdiction should prepare a security procedures manual. Since the completed manual will contain much sensitive information, strict control of all copies is important. In the wrong hands, this document provides information that can be used to defeat security measures.

Design

The following recommendations may be useful in developing a security procedures manual.⁵

Use a looseleaf binder. The binder had advantages over a permanently bound volume. The user can insert revisions or additional by substituting revised pages and discarding obsolete ones. In addition, cost is minimal comparatively.

Identify types of instructions and group by subject. Make it clear whether the policy or procedure being discussed is permanent or temporary. Permanent instructions have a continuing reference value and stay in the manual. Temporary instructions will be used a short time and destroyed,

⁴ Post and Kingsbury, 3rd ed., p. 666.

⁵ See General Services Administration, National Archives and Records Service, Office of Records Management, *Communicating Policy and Procedure, Records Management Handbook* (Washington, D.C.: General Services Administration, 1967), for useful suggestions on preparing a manual.

to help reduce the volume of material in the manual. Finally, grouping all instructions on a given subject in one place eliminates lengthy searching and reduces reliance on cross-referencing.

Number by a prearranged system. After choosing the manual subjects, assign numbers to them. The system used must be flexible enough to cover the various types of procedures, to distinguish between continuing instructions on the same subject, and to allow expansion of any one subject. Numbering each set of instructions will make a subject easier to locate, simplify control, establish a uniform sequence in the binder, and provide an automatic grouping by subject. The scheme selected should allow revisions as necessary.

Note that a device for identifying paragraphs is important to ensure accurate location. This can be done by numbering paragraphs and/or by indenting subordinate paragraphs.

Make the format standard. A standard format is needed because usually more than one person will be preparing the manual. This format will help readers find information and understand the relationships of different sections of the manual.

The heading for the first page of each set of procedures should include the agency or division issuing the instructions, a subject classification number, the effective date, the subject and any approvals needed. (For example, some procedures may require a court order.) The policy statement should be separated from and followed by the procedures to implement it. A suggested paragraph sequence would be: purpose (which includes the policy statement), procedures, and a list of attachments (such as forms).

Use reference aids. Aids that make the manual easier to use include cross-references, alphabetical subject index, numerical index, table of contents, tabbed divider sheets and copies of any forms used. The size of the manual should determine which, if any, of these aids is appropriate.

Date the instructions. Date each list of instructions to show when the list takes effect and to ensure that all manuals are current.

Schedule periodic review and revision. As conditions change, parts of the manual will need to be revised, so schedule a comprehensive review every year or two specifically to coincide with the effective dates of any recent legislative or judicial changes.

Avoid the following when revising the manual:

Unneeded supplements or those with separate paragraph numbers.

Instead, make revisions or additions to the original instructions.

Pen and ink changes. Avoid this because of the cost in time and the possibility for error or misunderstanding.

Paste-in changes. Often these are torn off and lost, so it is better to issue completely revised pages.

Establish master files. A background file of all instructions provides a continuous record of policies and procedures and an easy reference to cancelled or revised guidelines. Also keep a complete set of current procedures.

Include General Information

Key Personnel and Agencies. A list of emergency contacts should include names, titles and 24-hour telephone numbers. For easy reference, the following subheadings are recommended:

- Sheriff's office
- Police services
- Federal agencies
- Fire department
- Medical services: ambulance, hospital, doctors
- Judges
- Court administrator
- Clerk of the Court
- Building maintenance engineers
- Utility emergency services: gas, power, water, phone and cable
- Other courthouse tenants

Prepare a directory of building occupants, arranged alphabetically; by floor and/or office/suite number; and by agency and function. Schematic floor plans should show all occupants and include all openings such as doors, windows, service or access panels, and fire exits clearly identified. If possible, show in the drawing all utility control points, shut-off valves, elevator control panels, heating and air conditioning systems, firehouse and extinguisher locations, and emergency medical equipment. If this is not possible, attach a description of these locations to each floor plan.

Security Staff Organization and Post Assignments. An organizational chart of the security detail should be provided. In addition, the names and telephone numbers where officers can be reached at all times should also be included for ease of reference.

If security personnel are assigned to specific posts on a routine basis, draw up an instruction sheet for each post giving the following information: assignment area, duties, responsibilities, normal business hours, condition of doors and windows (i.e., locked, unlocked, open or closed), lights on or off in specific locations during and after normal business hours, and any special information for each post.

Regular Security Procedures

The next sections on the security procedures manual describe the more normal, non-emergency court activities and offer some day-to-day guidelines on the safety of judges, juries, witnesses, defendants and records. Note these sections occasionally repeat some of the material in earlier parts of this chapter. Obviously, some recommendations are appropriate under both emergency and routine situations.

Also note that the following sections often stress the court officer's role. Some jurisdictions may prefer to incorporate this kind of detail in a court officer's manual rather than in the security procedures manual.

Records and Evidence. The clerk of the court has primary responsibility for all material entered as evidence in court proceedings. This office is also responsible for the safety and security of all court records and related documents. However, the sheriff or court security officer can offer valuable professional advice on ways to improve overall security. Chapter 7 discusses some proposed structural measures if records and evidence storage areas are to be built or remodeled.

Several measures can ensure evidence security in jurisdictions that lack special facilities for this purpose.

- Reinforce a small closet in or near the courtroom. Provide a push-button combination lock. The clerk should change the combination periodically and keep it a secret.
- Use a large office safe.
- For more sensitive items, such as drugs and large sums of money, make arrangements with a local bank for use of the vault or a safety deposit box.
- Arrange to use space in the court treasurer's safe or vault.
- Access to any storage areas should be strictly controlled.

Records should be protected from tampering, theft and loss or damage by fire. The clerk's office needs a system of administrative controls when making files available to the court, attorneys or the general public. After-hours storage should be in controlled access rooms that can be locked and have fire protection devices, such as automatic sprinklers and alarms.

Judges. Protection for judges is usually minimal except in the case of an overt threat or when the possibility of danger exists. Everyday practices for judges' security include guarding parking spaces; assigning parking by number, rather than name; escorting them through public corridors; providing an alarm button in chambers; and searching those chambers daily for contraband.

Crank or threatening letters received by judges should always be forwarded to the sheriff or appropriate law enforcement official. Basic searches of chambers can be done by officers assisted by those more familiar with the routine contents of the chambers and able to identify suspect items quickly. Visitors are usually identified and screened by court officers, clerks or secretaries to ensure that they have legitimate business with the judges.

Judges are usually reluctant to have highly visible security measures instituted unless they are absolutely necessary. They fear that those measures might isolate them from the public and their constituency.

Higher levels of security for judges are discussed in the later sections in this chapter on high-risk trials.

Witnesses and Waiting Areas. Threats to witnesses often occur in the hallways before or after entry into court. These threats can be eliminated by providing separate witness waiting rooms for prosecution and defense witnesses. Admittance to these areas should be strictly controlled and access should be denied to all except witnesses, court staff and counsel.

Attempts also are made to frighten witnesses while they testify. Examples include reports of spectators making throat-cutting gestures or similar threatening

movements. The court officer should report any such occurrences to the judge, whom will usually order the person(s) removed or direct they be arrested.

More serious threats against witnesses or family members may require escort or bodyguard protections. If protection is required outside the courthouse, local law enforcement agencies may be called upon for assistance. Higher levels of security for witnesses are discussed later under high-risk trials.

Normal Jury Procedures. The conduct of court officers responsible for jury security is vitally important for the impartial administration of justice. The court officer must have precise instructions for handling juries, whether those rules are based on the guidelines recommended here or on statutory requirements.

This section of the procedures manual should give precise instructions for routine handling of juries. Court officer responsibilities for non-sequestered and sequestered jury security are discussed in detail in the next section of this chapter.

Jury Orientation. On their first day of appearance, all prospective jurors should be given a general orientation. Ideally, this would be a brief lecture by a judge or court officer. The orientation should outline what is expected of jurors and the responsibilities of the courts and court officers toward them. Points to emphasize include warnings not to converse with non jurors about a trial, the possibility of sequestration, and general measures to ensure the jurors' security. Court officers' jobs will be much easier if they have the cooperation and understanding of the jurors.

Site Viewing. When the judge decides a jury should leave the courtroom to view the scene of the crime or immovable evidence, the jury is normally escorted by the court officer or sheriff to the site, where a court-appointed person usually shows the jury the evidence. The escort officer is usually sworn: (1) to allow no one to communicate with the jury, which includes the court officer/court security officer as well, on any subject connected with the trial, and (2) to return the jurors to court without unnecessary delay or at a specified time. The site visit is a common occurrence in land condemnation cases, where it is necessary to separate jurors, lawyers and appraisers.

Custody During Deliberation. When attorneys have made final arguments, the judge will instruct the jurors, and then place them in the court officer's charge. The court officer is under oath to keep the jury together day and night, if necessary, and to abide by the communications restrictions mentioned under **Site Viewing**. Sequestered jury care is discussed later in this chapter.

For the benefit of women jurors, a female court officer, deputy or matron should be assigned during both day and evening hours. Jurors sequestered for the night are under the same restrictions as during the day, but they can send messages to their families through the court officer. Detailed notes should be given to the court officer, whom will relay the message by phone, keeping juror notes for the record.

Juror Illness. Court officers must know what to do when jurors become ill, especially when a juror may need to be hospitalized. Until the nature of the illness is known, it will be necessary to provide constant security for the juror, to make sure

communications restrictions are maintained. If the illness happens while the court is hearing testimony and a quick recovery is expected, the judge may adjourn the trial until the juror returns. Otherwise, the judge may replace the ill juror with an alternate.

If a juror becomes ill during deliberation or while sequestered, the court officer should notify the court immediately of any action taken. It is wise to have a list identifying doctors on call, an ambulance service and nearby hospitals with emergency facilities. Medical personnel should be cautioned to limit their conversation with the juror to the medical problem at hand. Finally, the court officer should prepare a report for the court describing any medical incidents involving jurors on a particular case.

Emergency Evacuation of Jurors from the Courtroom. Evacuation during a court session should happen only on the judge's order. The court officer is then responsible for moving the jurors to a predetermined place and assuring their safety. They will stay there until ordered to return to the court or to move to another location. During this time, the jury should be instructed not to discuss the case nor to speculate on why they were evacuated; the court will advise and instruct them on this issue when they return. It may also be necessary to isolate the jury from media information about their trial during this time.

If an emergency arises while jurors are in the courtroom but court is not in session, or while they are in the deliberation room, the court officer takes the same course of action as just described, consulting the judge first if possible. However, if the judge is not available, court officers should act on their own, notifying their superiors and the judge as soon as possible. If the jury is deliberating and has evidence in hand, the court officer is usually responsible for the security of that evidence and any notes or ballots until those materials can be turned over to the clerk of the court.

Jury Deliberation Room. This room should directly adjoin the courtroom or be nearby and only accessible by a restricted passageway. The room should be soundproof to prevent eavesdropping on the deliberation. The area also should be carefully examined before use and kept locked at all times. Jurors are locked in for deliberation and may summons the court officer at any time by means of a buzzer or knock on the door. All questions should be in writing to the judge, whom may write a response or direct the jury to return to court for further information and/or instructions.

The court officer should not communicate with jurors on any matters except to ask if they have reached a verdict. When the room is vacated, all notes and other materials used in deliberation should be removed and then safeguarded, destroyed or treated according to other established procedures.

Sequestered Juries. Sequestering juries is costly because jurors must be protected 24 hours a day, since security risks are much higher than in ordinary trials. Extreme caution is needed so that improper procedures do not result in a mistrial or provide grounds for reversing a decision in an appeal. The following guidelines will help simplify sheriffs' and court officers' jobs.

Security Plans. Security plans and procedures for each trial should agree with existing court rules and should be presented to the presiding judge for approval.

Deviations from the approved plans should be reported to the judge before they are carried out.

A supervisory court officer should be responsible for the jury and for security personnel assigned to the court officer. Such personnel should fully understand their duties and their relationships with jurors.

The court order for sequestration should discuss the conduct of jurors, plus appropriate restrictions and control measures (see Appendix B for a sample order). Violations or suspected violations of the court order or any suspected attempt to influence a juror should be reported to the judge immediately, and a written record made of the incident.

Personal Conduct of the Court officer. Court officers and security personnel should maintain a professional and courteous manner towards the jurors at all times. They should not discuss trial-related subjects nor allow others to do so, except by court order, and they should never express an opinion about the trial.

Access to Jurors. Access to juror's quarters should be given only to the security staff, those providing essential services or other persons authorized by the court. A visitor's identity, purpose of visit and time of arrival and departure should be recorded in a log. Written authorizations for visits should be retained for the record, and entries should be made in the log for verbal authorizations.

Service personnel, such as waiters and cleaning staff, should be logged in and accompanied by a court officer at all times while in the jurors' quarters. They should not talk to jurors. It is also a good practice to find out if any of the service personnel are related to trial participants. Finally, jurors' laundry should be inspected by the court officer before it is sent out and before being returned to the jurors.

Accommodations and Meals. Some officers argue that arrangements for meals and quarters for sequestered juries should be their responsibility because they are most aware of security requirements. Others believe this is mainly an administrative function more properly performed by the trial clerk, with some guidance from the security staff. If security makes these arrangements, they should select hotels, restaurants and other accommodations fairly, impartially and based solely on security considerations.

To maintain security and control, hotels are better than motels because the court can get a block of rooms on a single floor that is isolated from the general public. An upper floor in the building is best, to reduce the possibility of communications from outside sources. The following recommended guidelines should then be followed:

- Remove or disable television sets, radios, computers and any electronic device that provides Internet access in jurors' rooms.
- Control telephones so there are no unmonitored incoming or outgoing calls.
- Generally assign two persons to a room, with the sexes kept separate.
- If a private dining room is not available, use a spare room on the jury floor for meals. Escort jurors from the dining room to restrooms.
- At the discretion of the court, jurors may have a limited number of cocktails in the evening – usually two – at their own expense and only if they are not

returning to court or deliberations that evening. Court officers should never drink alcoholic beverages while on duty.

- Keep accurate financial records of meals, according to the court's standard procedures and payment policies.

Transporting Juries. During transportation to and from the courthouse, jurors are subject to possible physical harm and outside influences. If there is some reason to suspect an attempt on the jurors' physical well-being, an advance security force should scout the route and recommend detours or other tactics.

Precautions are needed to make sure the jurors do not see newspapers, posters, banners and the like during the trip. Transport vehicle should be searched in advance for such materials, and jurors should not hear commercial radio broadcasts nor walk by newsstands or newspaper dispensers. It may even be necessary to cover vehicle windows with opaque material to keep jurors from accidentally seeing newspapers or similar materials.

Drivers should be told not to talk to jurors at all about the trial, and escort officers will need to prevent jurors from being interviewed during transport.

Emergency Evacuation from Sequestration Site. In case of fire, bomb threat or any other emergency situation that might harm jurors, the court officer should immediately evacuate them to a predetermined location. As mentioned before, jurors need not be informed of the reason for the move, only that it is necessary; they should be cautioned not to discuss the move or speculate as to the reason for it.

Whenever a jury is sequestered or retired for the night during deliberations, suitable transportation should be available on a standby basis in case an emergency arises.

Access to Media. Court orders should specify which types of media sequestered jurors may see and hear, if any. If authorized, a television may be set up in a common lounge; however, the court officer ought to monitor the set continually and turn off scheduled newscasts, bulletins and captions. Programs the jurors watch should not have a theme similar to the case being tried. If possible, videotapes can be made to ensure that no unauthorized material is seen, and there should be a record of all programs viewed. The television set controls should be locked when not in use or when the room is unoccupied, and jurors may not have radio receivers or transmitters.

The court may approve newspapers, magazines, periodicals and books for the jury's use, provided those materials are censored first and records are kept showing the items made available. Preferably two persons should review the publications beforehand, removing and filing any material about the trial or similar incidents.

Communications with Others. Occasionally the court may permit visits between jurors and family members on weekends or off-duty days. A record should be kept of all visitors, and a court officer should be present to make sure there is no conversation on trial-related matters.

Only court-authorized telephone calls should be permitted. These calls should be dialed and monitored from the court officer's room using special phones with monitoring

features, which the telephone company usually can provide. Court officers should dial the numbers, identify themselves, warn the answering parties not to discuss the case, and advise both parties that the call is being monitored and will be terminated immediately if the warning is not heeded. Incoming calls should be handled similarly, after they are directed to the court officers' stations. Court officers should keep logs of all incoming and outgoing calls.

All mail and packages should be given to the court officer for examination and censoring before they go to the jurors. Likewise, outgoing mail should be censored before mailing. If jurors do not agree to this procedure in writing, their mail may be withheld until the end of the case, or as ordered by the court.

During a prolonged trial, the judge may permit recreational trips, attendance at religious services, shopping or business meetings. If so, recreational areas should be secluded and adequately protected. Clergy should be advised in advance of a juror's attendance and asked not to mention the trial in the service. Business meetings should be conducted only under close and constant security. Generally, the court officer should do all shopping for jurors, being sure to keep a written record of expenses and money received. If allowed to shop for themselves, jurors must be under close supervision.

The court may authorize barber or hairdresser services. If possible, this should be done in the juror's room and under close supervision, with service people advised not to discuss the trial. In a shop, the court officer should be sure the juror has no access to newspapers or publications that have information about the trial.

Medical Services. It is wise to have a first aid kit available at the sequestration site. The court should be advised of the medications prescribed for jurors, possible medical problems, and medication that might be required. Otherwise, the medical procedures here are similar to those mentioned before under **Juror Illness**.

Records and Forms. Many materials are needed to document the care and safekeeping of a sequestered jury.

Handling In-custody Defendants. Incustody persons appearing in court generally fall into one of three (3) categories: (1) defendants being tried or sentenced, (2) prisoners being tried for additional offenses committed while in prison, or (3) prisoners appearing as witnesses. People in custody think of escape at one time or another, and convicted felons serving lengthy sentences often are preoccupied with thoughts of escape.

An analysis of the custodial system shows the weakest link – the most likely time for escape attempts – is when the person is outside the correctional facility. This means during transport from the jail or other correctional facility to courthouse, in the temporary holding area, and in the courtroom. During these times, the jail or correctional facility's custodial force is replaced by a limited number of transportation officers and court officers. The prisoner is usually guarded by only one court officer, whom is often occupied with many other trial-related duties.

Movement To and From Jail/Correctional Facility. If a secure tunnel or bridge is not available for movement between the jail/correctional facility and court, a vehicle should be used – even for short distances. Movement by foot through public areas increases the risk of an escape attempt and also makes the security force and individual(s) in custody

vulnerable to attack. All transport vehicles should be properly marked and should contain standard emergency equipment, such as portable lights, fire extinguishers, first aid kits, tear gas dispensers, flares and communications gear. Transport vehicles should be searched for contraband before loading the in custody individual. High-risk trials may call for additional precautions, as discussed under that section of this chapter.

In custody individuals should be placed in restraint devices before leaving jail, and the devices should be removed in the temporary holding area within the courthouse. If such an area is not available, restraints should be removed immediately before the in custody individuals are taken into the courtroom and replaced immediately after they leave.

Weapons should not be worn by officers directly handling prisoners. They may be worn if more than one person is guarding the individual(s) in custody; however, the armed guard should always be in a position to avoid being overpowered and disarmed. A single officer should never be required to move more than one in custody individual at a time.

Temporary Holding Areas. Temporary holding areas should be designed to confine in custody persons and reduce escape attempts, but should not have features that violate an individual's constitutional rights. For instance, temporary holding areas should have separate facilities for juvenile and female individuals, as well as space to provide various degrees of isolation and protection. Female deputies or matrons can be assigned to observe in custody females and search them when necessary.

In the holding area, security personnel should search in custody individuals when they arrive from a custodial institution and before they are returned. In custody individuals are not to have any personal property other than any legal materials pertaining to their case. Moreover, there should be clear rules and instructions on monitoring and on dealing with escapes. Temporary holding areas should be examined daily for the soundness of walls, floors, doors and windows, as well as adequate ventilation.

Segregation of Hostile Groups of Prisoners. Court officers and security officers should be aware of possible serious problems which could develop between prisoners, if hostile factions are not segregated in the holding areas and the courtroom. An example is if an informant appears as a witness and members of hostile gangs appearing as defendants in the same case. Vigilance must be maintained in the courtroom, where witnesses may be the object of attack. Trials with several defendants also may involve problems among the defendants.

Movement of individuals in custody should be planned so that hostile factions do not come into contact, even while passing in a corridor. Well-planned movements will reduce opportunities for threats or physical violence.

Appearance and Control in Court. The possibility of an escape attempt from the courtroom should always influence the actions of court officers and security personnel. If there is reason to believe a prisoner will try to escape or resort to violence or unruly conduct, the court officer should stay behind the prisoner to provide better control.

In cases where a prisoner or group of prisoners presents an unusual security risk, the judge should always be advised, and additional courtroom security measures can be

suggested for the judge's approval. Permission is needed to keep the in custody individual in restraints in the courtroom, and usually only unobtrusive restraints will be approved in jury trials. Some courtrooms have dealt with this problem by providing special chairs at the defense table and the witness stand. (*See* Chapter 7 for more on these chairs.)

Escape Attempts. A simple plan is needed to deal with escape attempts. Most attempts are spontaneous and triggered by apparent weaknesses in the security system; they usually happen in one of these four places while in custody individuals are away from the jail/correctional facility:

1. Transit between jail/correctional facility and courthouse;
2. Public hallways;
3. Courtroom; or
4. Temporary holding area.

Specific plans to deal with escapes depend almost exclusively on the physical layout and manpower resources of each court. Also, each location presents different problems and requires advance planning to reduce successful escapes. However, basic procedures can be developed, including the following:

- *Activate an alarm.* If the attempt is made in the courtroom, the clerk or judge should activate the alarm, since the court officer will be in pursuit. In the holding and other secured areas and in public hallways, a police whistle can be used to alert other security personnel, whom can join the pursuit or go to prearranged posts to secure doors and try to catch the escapee.
- *Notify key people.* The clerk should notify the security officer in charge, whom, in turn, should notify the sheriff. If the individual is not caught immediately, state and local police agencies should be given complete details, including a physical description. These agencies should have plans to establish roadblocks and surveillance of possible escape routes.

Fire and Bomb Threats. The security office should have a policy on handling in custody defendants in the case of fires or bomb threats. Usually, the in custody individuals should not be removed from holding facilities unless an immediate threat exists. If removal is necessary, full restraints should be used and adequate personnel assigned. Deputies assigned to this duty should be vigilant for possible escape attempts, since the threat may be a hoax designed to aid an escape. In custody individuals should be returned to the detention facility as soon as the area has been thoroughly searched.

Medical Treatment. A physician should be on call to provide medical aid to in custody defendants when necessary. In custody individuals removed from holding cells for transportation to or from medical facilities should be under restraints, and transport officers should be alert to possible escape attempts.

Policy on Restraining Devices. This policy should be set by the sheriff and uniformly applied to all prisoners. The policy should include minimum levels of

restraint, such as handcuffs, leg irons and restraint belts or chains. Having a policy eliminates the need for each officer to make decisions in this area. However, individual judges must also be consulted because many have their own policies on restraints in their courtrooms. Finally, deviation from established policy should be only by court order or with approval of a competent authority. A written record of any deviations should give complete details.

Guidelines for Disruptive Conduct. As noted in Chapter 2, the United States Supreme Court has issued guidelines for handling unruly criminal defendants in the courtroom.⁶ When defendants are so disorderly that their trials cannot proceed, the court has three alternatives: cite them for contempt, shackle and gag them, or remove them from the courtroom.

The Supreme Court held that shackling and gagging should only be used as a last resort because such action prejudices a defendant in the eyes of the jury and offends the dignity of the court. Removing defendants from the courtroom is preferable to binding and gagging, though the defendants must first be warned that they will be removed if the disruptive conduct continues. Once removed, they should be allowed to remain nearby to consult with attorneys and should receive a standing offer to return if their conduct improves.

A secure, soundproof holding room should be next to the courtroom for the use of defendants removed for being disorderly. Many courts already provide such rooms for the custody of incarcerated witnesses waiting to testify and for defendants during recess. Closed-circuit television or a loudspeaker will allow the defendant to see or hear the proceedings.

Finally, in the courtroom, telephones or duress alarms should be available for the court officer, clerk or judge to summons help in case of a serious disturbance by in custody individuals.

Policy on Communications with Others. Particular care must be taken to prevent unauthorized communications by or with in custody defendants, or attempts at such communications. Both actions are usually illegal, and many courts post notices to this effect, citing possible penalties. Defendants may confer with their attorneys in the courtroom with the consent of the court, but should do so in a manner that will not disturb the proceedings. No other persons are allowed to visit a prisoner in court without the judge's permission. A person in custody should never be allowed to accept any money, clothing or other items directly from anyone in court, such items should be presented to the jail for control and examination for contraband.

Attorney-Client Conference. Attorney-client conference areas adjacent to the courtroom holding rooms allow attorneys and clients or witnesses to discuss testimony and a case's progress. These are restricted areas, and must be secure enough to prevent escapes. Before and after use, the rooms should be searched for contraband, especially when the court has allowed visits by relatives and friends.

⁶ *Illinois v. Allen*, 397 U.S. 337 (1970).

Multidefendant Trials. The special circumstances of trials with several defendants may require additional security precautions. These should be discussed with judges, who can approve any recommendations or issue court orders if necessary. Multidefendant trials generally mean more security manpower; normally, there should be one court officer or security officer for each defendant. In the courtroom, these officers should be positioned to prevent an escape attempt or to control each prisoner in case of a disturbance. Note that defendants may be antagonistic towards one another and may require segregated seating.

Female Defendants. Female defendants should be subject to the same policy approved for males regarding use of restraining devices. If separate policies are in force, they should be clearly defined and in writing. Uniform application of restraints on all prisoners regardless of sex will reduce unrest and charges of favoring some groups. Any deviation from this policy should be made only with the approval of a competent authority and also made a matter of record. Some departments may have a modified policy for use of restraints on female prisoners. However, security personnel are reminded that female prisoners can be just as dangerous as their male counterparts, and they too commit acts of violence, causing serious injury to themselves or the custodians.

If there is no separate temporary holding area for females, they may be held in the courtroom. These defendants should be seated close to the court officer's station, where they can be kept under constant observation and control. If a female deputy, court officer or matron is not available, at least two male officers should be present at all times to reduce or prevent charges of an individual's misconduct towards a female in custody.

Juveniles. As noted in Chapter 2, security officers must be constantly alert in these cases, since incidents caused by juveniles are usually unpredictable. Many juvenile court incidents are sudden outbursts of anger, often directed toward parents, or they may involve an attempt to escape.

Court officers and security officers should not view juveniles as merely underage adults to be handled like adult offenders. True, many youths are clever, cunning and very intelligent, but there are also many whose delinquent behavior can be directly linked to a serious learning problem, a low IQ, or an emotional disturbance. Usually, one of these factors has caused the conduct that brought the juvenile into court.

It is important to identify children whom may have emotional or learning problems. Case workers and probation officers should take the time to develop data from schools, medical records and other sources. If these problems exist, the court officer and correctional staff should be told in order to help them decide how to deal with the young people involved.

Children with these problems will usually respond to a situation they cannot understand or cope with either by silence or a violent reaction. Fear of the unknown should be met with reassurance, through communication with a court officer who has special training and the right attitude. The court officer should be both sensitive to the special problem child and also aware of the possibility of being deceived by the "streetwise" offender.

Mentally Ill Persons. On occasion, the mentally ill must appear in court. Thus, court officers need to be emotionally mature people whom can cope successfully with unusual

behavior. In each instance, a check with institutional officials is important to find out what behavior to expect. There may be special requirements for straitjackets or seat pads, or cleaning materials to handle someone who spits or drools. It is advisable and often mandatory that a doctor or medical attendant be present at these appearances.

Court officers should be attentive and give these people as much assurance as possible. If they show violent or erratic behavior, the court officer must subdue them and call for any necessary help from medical attendants. Court officers should be aware that these patients might exhibit strange and unpredictable behavior and may not respond to the usual warnings.

Handicapped Defendants. Particular care is needed with handicapped defendants, and any improper conduct by the court officer may prejudice the case in the eyes of the jury and cause a reprimand from the judge. Deaf-mutes, for instance, require a high degree of visual contact with the court officer to assure compliance with instructions. Another special concern is how restraints are used, for both the prisoner's condition and the need to assure proper control are important.

Particular attention is advised when searching handicapped persons for contraband. Also, sympathy for the handicapped should not mean reduced vigilance, for even a crutch can be a formidable weapon in the hands of a determined person.

In handling a handicapped defendant, the best advice is "plan ahead." Security staff will also need to plan ahead if the nature of a person's infirmity is such that medical attention may be needed. Inability to handle the unexpected always creates a weak security operation.

Defendants Representing Themselves.⁷ In 1975, the United States Supreme Court affirmed the right of defendants to represent themselves if they understand the nature of the charges against them.⁸ Thus, court officers must be familiar with certain privileges for incustody defendants whom act as their own lawyers. Each jurisdiction should form a committee of judges, prosecutors, sheriff's representatives and others to draft policy on *pro se* defendants both in jail/correctional facility and in court.

San Diego County has dealt with these permitted privileges in some detail.⁹ There, the presiding judge of the superior court approved the following recommendations of a judge's executive committee dealing with *pro se* defendants in jail:

- Provide case-related work areas for the defendants;
- Provide books, supplies (e.g., subpoena forms) and equipment (e.g., tape recorders);
- Allow the defendant use of the jail library, telephone privileges and interview with witnesses;
- Allow the defendant to receive mail related to the case;
- Make provisions for legal researchers and investigators, spelling out how they will be assigned and paid; and
- Provide for suspension of the above privileges when necessary.

⁷ The legal term here is *in propria persona* (*pro per*) or *pro se*.

⁸ *Faretta v. California*, 415 U.S. 975.

⁹ San Diego County Sheriff's Department, Court Services Operations, *Superior Court Court officer's Manual* (San Diego, California, 1977).

When defendants act as their own lawyers in court, there are unique security problems. In cases where dangerous weapons are introduced into evidence, the court may rule that defendants, even though representing themselves, may not touch the evidence. In addition, *pro se* defendants should be required to maintain a safe, specified distance from juries, witnesses, court personnel and observers.

Special Courtroom Considerations. During the judicial process, there are times when the potential for incidents is greater than usual. At these critical periods, the court officers and security officers should be alert to the possibility of disruptions or escape attempts. A few of the critical times already discussed in this chapter include: (1) the appearance of an antagonistic witness or codefendant; (2) prisoner movement to and from jail/correctional facility, or between temporary holding areas and the court; and (3) appearances involving juveniles.

Other critical times to address in the procedures manual are include below. In these situations, incidents will usually be in the form of a physical assault, possibly coupled with an escape attempt.

- During arraignment and sentencing;
- When a verdict is rendered in a domestic or small claims court;
- During convening of a psychiatric court;
- When dealing with unruly spectators;
- When litigants or defendants, who are on bond, bring weapons into court because they were not properly searched.

Arraignment and Sentencing. Arraignment and sentencing are often hectic times. Large numbers of lawyers, friends and relatives are present, along with both incustody defendants and those on bail. If the court revokes bail or sentences someone, there is an abrupt separation of defendants from relatives. Emotions will often run high, for example, as a wife tries to have “one last talk” with her husband before he is taken away. Defendants not expecting to be confined frequently are shocked into violent outbursts, and unless the overall situation is well controlled, the courtroom will be the scene of general disorder. The need for more than one court officer or security officer at this time is obvious.

Civil and Domestic Court. Because violence occurs more often in civil and domestic than in criminal courts, court officers should be specially trained for those types of problems. Emotions peak, for example, when rulings are made on separations, divorces and custody of children. The disappointed person may use a firearm on an attorney or the successful litigant. In Florida, a woman who lost her house in a suit took a gun from her purse and killed her adversary before a horrified judge and spectators.

Small Claims Court. Many assaults are committed in small claims courts, usually at the time of a decision. Many jurisdictions now notify litigants of small claims decisions by mail to avoid the often violent reaction of the loser. Court officers or security officers in small claims courts must be aware of the types of problems that can occur and be prepared to handle them.

Psychiatric Court. Psychiatric courts are convened to hear a number of matters: defendant's mental competence to stand trial; defendant's addiction(s); and whether or not a defendant is predisposed, by reason of a mental illness, to commit sexual or other crimes. This court may also hear civil matters (e.g., putting people in the care of conservators appointed to look after their interest.) In certain instances, because of a defendant's condition, the court may convene a bedside hearing, which is governed by normal courtroom procedures.

Court officers in psychiatric courts must be sensitive to the needs of mentally disturbed persons, must give people assurance during the proceedings and must recognize the fact that violent or erratic behavior can be expected during a hearing.

Unruly Spectators. There is a danger of overreaction in dealing with unruly spectators, and this response could make an otherwise minor and controllable incident more serious. In most cases, a simple warning by the court officer or judge will control the situation. In some instances, the court officer may be instructed to bring the offender to the bench, where the judge issues a warning and explains the consequences of further unruly conduct.

Judges and their court officers usually have an "understanding" on how these matters will be handled. Many judges will try to give the unruly spectator the benefit of the doubt and every opportunity to correct his/her behavior. Some disruptive incidents are committed by people with mental disorders and require an appropriate response. If a person's conduct does require removal from the courtroom, such action should be taken quickly.

Searches of Litigants and Defendants on Bond. Many serious incidents have occurred because weapons were brought into the courtroom. Thus, discreet searches of litigants and on-bond defendants are needed before they enter the courtroom, especially for trials involving highly emotional situations. However, this search requirement is a sensitive issue, and a clear policy on the matter obviously is needed. This means looking at the issue's legal aspects and getting both guidance and approval from the presiding judge.

Factors Influencing Disruptive/Unacceptable Behavior. Factors which contribute to disruption in court include those identified below. Many of these factors can be recognized and addressed by a change in attitude and conduct or by increased security awareness and suitable precautions.

- Attitude and conduct of both judge and court officer;
- Prosecution tactics;
- Presence in court of friends or relatives of the victim or defendant;
- Damaging testimony;
- Dissatisfaction with defense attorney's conduct of the case;
- Unwillingness of defendant to accept the court's authority;
- Values or political beliefs of the defendant(s);
- Desire to gain publicity for either an individual or a cause;
- Mental instability;

- Fear of confinement; or
- Sentencing to a long prison term.

Special Operations Plans

Search of Courtroom(s) and Related Space. A thorough, systematic search of these areas by trained personnel should be mandatory both before and after the court convenes. Trained officers can quickly identify locations where contraband is likely to be hidden. In particular, areas near the defendant should be thoroughly searched. After finding one piece of contraband, the searchers should not stop their work nor relax their vigilance, for there may be more. Any suspicious items found should not be moved or handled until technicians have had the opportunity to check for fingerprints or other evidence. After the courtroom is searched before its use, the room should be under constant surveillance by the court officer or security officer until the proceedings start.

Judge's secretaries often can help search judges' chambers because they are familiar with the area and can quickly identify strange or unusual items. However, primary responsibility for conducting searches should remain with the security officer.

Visitor Control. The simplest way to control visitor movement is to provide easily read directories and floor plans at building entrances and by elevators, in addition to well-marked corridors and office doors. Another measure is an information or reception desk staffed by a civilian who can serve as a lookout for potential problems and warn security officers of any troublesome or potentially disruptive people entering the building.

Under normal conditions, courthouses are freely accessible to the public. However, access to certain areas, such as judges' chambers, should be controlled at all times through either architectural design, locked doors or guarded checkpoints. Sometimes it might be necessary to control entrances to the building or courtroom, perhaps including package searches or the use of metal detectors, -- tactics commonly referred to as a "search screen." However, these measures should not be applied indiscriminately because they might be challenged on the grounds of prejudice to individual rights. Usually a court order is required for these procedures, and that order should be prominently displayed for public examination.

Basically, a search screen identifies those admitted to the courtroom and locates contraband and metal objects which may be used as weapons. General recommendations for a search screen operation include the following:

- A barrier should isolate the operation from the general public.
- A minimum of three security officers is recommended for processing spectators.
- A female officer or matron should be part of the team.

Depending on the anticipated risk, any or all of the following elements may be used in a search screen.

- *Receiving or starting point.* All persons enter at a certain point controlled by a uniformed officer. If body or metal detector searches are part of the screen, people empty their pockets into containers and purses are inspected or emptied.

- *Search booths.* Two booths are recommended, one staffed by a male and the other by a female officer. Within the booth, the officer examines the personal belongings in the container and does a close body search.
- *Metal detector (magnetometer) station.* A walk-through magnetometer is desirable, though a hand-held model may be used instead. After examination, people may re-pocket all personal property except contraband and possibly identification but only until the search screen process is completed.
- *Photography station.* A technician should photograph all court spectators and their identification documents.
- *Seat assignment and recording.* A uniformed officer should identify and record information about all persons entering the courtroom and should assign seats based on a seating chart. Identification, such as a driver's license, may be retained by the officer, with the assigned seat number attached to make re-admittance easy after a recess. While escorting spectators to their seats, the officer should warn them that if they move to an unassigned seat they may be removed from the courtroom and that they will not be able to return if they leave the courtroom at any time except during recess.

Hostage Situations

Although hostage taking is rare, it is nevertheless a contemporary criminal tactic, and must be considered as a potential means of escape once a person is brought to trial. Being prepared for a hostage event will prevent overreaction that might endanger the lives of the hostages as well as security personnel.

A defendant's choice of a hostage will generally depend on whoever is most convenient, but an armed court officer may be particularly favored because the court officer's weapon can aid an escape. Spectators who take hostages generally bring weapons into court, though good screening could prevent this. High-risk trials have great potential for incidents involving hostages. Therefore, the importance of gathering intelligence cannot be overemphasized in planning the right response to prevent violence from defendants or their supporters in the spectator group. Following is a discussion of preventive actions and training programs for security personnel to consider as a response to hostage incidents.

Being Prepared

There are three phases in the hostage control program. The first is the *pre-event phase*, when planning occurs, administrators make sure that people are trained and the right equipment is available. The second phase is the *event* itself, when the plan is put into effect. The third is the *post-event period*, when those who carried out the plan evaluate how well it worked.

Many law enforcement agencies do not have the special skills and resources needed to deal with hostage situations and will need help. In many cases, nearby larger sheriff's or city police departments, or perhaps the state police, will have contingency plans and trained hostage negotiators. In other cases, the FBI may be able to help. However, in some areas no one force will have these resources; thus, polling and

coordination among law enforcement organizations will be needed. This section offers general guidelines that individual departments or regions can tailor to their needs when help must come from outside the department.

Pre-event Actions. Joint planning by two or more law enforcement agencies (the response force) should be geared to producing an “operations plan” for a hostage situation. The following elements should be part of that plan.

Policies and Objectives. Critical are policies on how members of the response force will work together. These policies are especially important where the resources of one group will be used in the legally defined jurisdiction of another. Thus, matters of liability and responsibility should be considered. In addition, the following are some key policy questions to ask on what will and will not be negotiable:

- Should captors be allowed to leave the courthouse? Should they be given transport away from the courthouse with the hostage? Without?
- Should an exchange of hostages be allowed? What other demands (e.g., for weapons or more hostages) should be met? What is the right response in these cases?
- Should food, drink, cigarettes, etc. be provided to captors?
- If hostage takers demand interviews with the press or want to publish “manifestos” about their grievances, should the press be allowed or encouraged to go along with these demands? Also, what is the relationship between the press and security forces?

Large departments with hostage experience have formulated policies to deal with some of these questions. For example:

Movement of the captors to another location is negotiable.

Except when a vehicle and driver are provided to move the captor to another location, another person is never substituted for the hostage.

Food, drink, cigarettes, etc. are given captors in exchange for concessions.

Press interviews are sometimes allowed after the release of the hostage.

These are usually permitted only if they were promised to the captor by the negotiator, or if the commander promised interviews to the press.

Press cooperation is a must.

The policy that results from answering these kinds of questions should be consistent with the primary objectives of the hostage plan. The negotiator must fully understand the policy, which also should be included in the training program for members of the hostage control group. Obviously, certain sensitive details about the policy should not become common knowledge nor be given to the press.

Initial Contact Procedures. The hostage plan should identify the people to be notified when a hostage event takes place, including both office and home telephone numbers for those people. The sheriff, commanders of other police forces involved, and possible political officials (who may be notified by the sheriff directly) should be on this list.

Responsibilities. The plan identifies the main person (and an alternate) who will direct the operation and run the control center. This person will decide on actions during the negotiation stages and will bring together all the resources needed to deal with the event.

Joint Force Coordination. The plan also describes the roles of each cooperating law enforcement agency. Usually, a sheriff will be the first to learn about a problem in the courthouse or courtroom. The sheriff may then assume the role of overall commander, with help from outside resources. Another alternative is an assisting force may be asked to control the operation, with the sheriff helping in various ways (for example, securing the outer perimeter). Decisions on the most effective use of manpower will depend on the capabilities of the various departments involved.

Equipment, Materials and Training. Examples of what may be needed are communications and personal protection equipment, electronic sensors and special weapons. Further, the response forces should be trained to use such equipment. Also needed are floor plans of the courthouse and enlargements of any courtrooms involved in the hostage incident.

Once the plan is final, personnel can be assigned from the law enforcement agencies involved. Some departments prefer officers who have served in the military, since they are accustomed to the high level of discipline required. These people should have intensive training, including field exercises, in the plan and its operation. This joint training can build up trust between departments: that trust is an intangible benefit that adds to the chances of success in a hostage case.

The Event. To the extent possible, the contingency plan will anticipate what is needed for an effective response. However, each hostage situation is different, and good plans will reflect the need for commanders to make decisions on the spot. Thus, the control officer's job is extremely important.

At first, the overall commander, usually the sheriff, will be responsible for confining the captor to as small a space as possible and preventing an escape. The sheriff will want to ensure that firearms discipline is maintained, and no one acts independent of the team. At the outset, the sheriff will be concerned with the inner perimeter. The sheriff will determine whether to evacuate or not, and, if so, how much. The sheriff will put the contingency plan in motion by relaying all information about the event to the joint force commander, the appropriate political official and the control center commander.

Control Center. The control center commander and assisting staff are stationed in this pre-designated communications area. The control center commander will do the following:

- Inform the response force commanders of the operation's status and receive guidance from them;
- Inform political officials and receive guidance from them (the sheriff could do this if desired);
- Maintain contact with the negotiator and offer information and advice;
- Receive intelligence from various department sources;

- Keep the press officer informed so that he or she can provide appropriate information to the media;
- Receive technical assistance from the psychologist, if one is involved; and
- Through the mobilization center (described later), direct the use of manpower for special details not included in the operations plan.

Negotiator. The purpose of negotiations is to save human life by buying time through the use of people trained in the psychological techniques of hostage negotiations.¹⁰ Time is the important factor for, as a rule, the more time captors spend with hostages the less likely they are to kill them.

Experience shows that the best negotiators are those who have had street experience during their law enforcement careers. Negotiators should look mature, so the captors will see them as people with authority. However, negotiators should not portray themselves as the final decision makers; thus, they will be able to defer decisions and gain time. When demands are delayed or refused, a relationship can be maintained because the negotiator is not the person denying the captor's request.

Negotiators must be able to communicate with captors. The ability to use informal or "street" language and to sympathize with the captors' problems is helpful. The negotiator should be the only person allowed to talk to the captor, except when an agreed-upon demand involves someone else (a captor's family member, for example).

Mobilization Center. This is a predesignated point where manpower from the various forces begin work. Here briefings, assignments, and equipment can be obtained. The commander of this center receives instructions from the control center commander for special details and provides the necessary support (such as specially equipped vehicles or food and drink).

Press Officer. The news media are an important element in any hostage incident. Unfortunately, experience shows that the media can become a problem in these situations. Thus, it is important to assure that media needs are met, while preventing reporters from intruding into efforts to release the hostage safely.

Information should be made available to the news media by the control center commander through the press officer. In nearly all cases, the security force operation will not be helped by media people who try to get interviews or television footage of captors and hostages. The key concerns, then, are what will help get the hostage released safely, and also what can be done to help meet media needs. The press officer's role thus becomes very important. It also would be helpful to: (1) discuss with media representatives those aspects of the contingency plan that affect the media; and (2) try to gain cooperation before an incident occurs.

Perimeters. The outer perimeter is loosely defined in an actual hostage situation, but generally surrounds an area where only security personnel are allowed. The inner perimeter marks an area that only the negotiator and the containment/assault team can enter.

¹⁰ New York City Police Department, *Tactical Manual for Hostage Situations* (New York: New York City Police Department, undated), p.6.

Postevent Actions. Officials often overlook the significance of the post event period. After a hostage case, certain actions are important, as discussed in this section.

News Release. All persons involved in the event should help prepare a news release, so the complete story is available to the public. The story may be released by the sheriff, a political official, or someone else, but it should be complete, factual and accurate.

Critique. Officials who participated in the event should review the following: all security force actions and how well prepared the forces were for each; the contingency plan and any changes needed in it; all policies on hostage incidents; and the effectiveness of the training plan for those situations.

Officials who participated in the event should write a report on the incident, describing in detail both the situation and response. This report should go to the political officials concerned, the sheriff, and the chief administrators of any outside resources involved.

High-Risk Trials

A high-risk trial is one that provokes a strong emotional response from the general public or interested groups. That response may threaten the safety of those involved or lessen the integrity of the judicial process. Thus, special efforts are needed to make high-risk trials safe, fair and open. To do this, courts need a well-organized, detailed operating plan.

The following elements of an operational plan are drawn from one that the Los Angeles County Sheriff's Department uses.¹¹ All these elements should be included in high-risk trial planning; however, some may have to be changed, based on the size of the sheriff's department and available resources.

Responsibilities and Coordination. One officer should be in charge and have full authority and responsibility for the operation, though a second in command can help if the unit is large. The commanding officer should control special communications and monitor the performance and conduct of assigned personnel. As a member of a special security committee, the commander helps design the operational plan and coordinates the work of all agencies involved (sheriff's office, state and local police, federal agencies, court, fire and medical units, etc.).

The commanding officer and the trial judge may be the only members of the security committee, though larger jurisdictions may add the presiding judge, court administrator and people from other law enforcement and emergency aid agencies.

Along with its coordinating job, the security committee also establishes policy and procedures, such as the right amount of security for juries, special precautions in handling high-risk defendants, and the level of security to be imposed for entry into the

¹¹ Los Angeles County Sheriff's Department, Civic Center Security Unit, *Major Security Trial Operation* (Los Angeles, undated).

courthouse and courtroom. Finally, the committee selects a suitable courtroom and drafts the necessary court orders to take all the steps just mentioned.

Personnel. High-risk trial security operations take place under stressful conditions. Thus, it is important that well-trained, physically able and mentally alert personnel be assigned to those duties. High marksmanship standards are also important. Role playing and “walk-through” exercises (mock drills) are needed until the commander is satisfied that officers know their assignments. In addition, clear-cut instructions should be written to outline the duties for each post in the plan. These instructions should guide individual conduct for normal, as well as emergency, situations.

Intelligence and Communication. Good intelligence information is vital to an operational plan. Court security staff should collect and analyze data for trends or indicators that might affect overall security planning. Such trends could appear, for instance, in disrupted trials involving defendants with similar backgrounds or group affiliations. Information on those cases might help identify the disruptive followers or associates of the defendant so that court personnel could be alert to their presence. Such data are available from court and departmental records, the news media, criminal records systems, and various law enforcement agencies. In trials with a change of venue, the sheriff’s office or original jurisdiction may have much of this information already collected.

Along with intelligence, communication is vital to an effective operational plan, and efficiency is reduced if one part of the security system cannot communicate readily with another. All communications should tie into the command center, which can be a specifically created post or the sheriff’s radio dispatch room.

Arrest and Reporting Procedures. Procedures for making and reporting on arrests should be worked out in advance. For instance, when multiple arrests are expected, procedures must be well-defined and approved by the court in advance. This kind of planning can keep those arrests from being invalidated on appeal and helps prevent suits for false arrest. Good intelligence also should indicate whether or not multiple arrests are likely to happen.

Courthouse and Perimeter Security. For high-risk trials, 24-hour security coverage of the court building and its surrounding area is recommended. During normal business hours, expected threats would be disruptive demonstrations, mass movement into the courthouse and courtroom, and efforts to bring contraband into the building. After-hours threats would most likely be attempts at surreptitious entry for destructive purpose.

When the courthouse is open, the following measures are advised to ensure security in the courthouse and perimeter:

- Patrol the outside of the building.
- Provide guards for judges and jury parking.
- Inspect shrubbery and other places where explosives or contraband could be hidden.
- Monitor all entrances.

- Patrol inside the court building, especially public areas near courtrooms.
- Frequently check basement, engineering spaces, heating and air-conditioning equipment, and potential entry points such as roof openings, utility tunnels and locked doors and windows.
- Equip all patrol units with two-way radios to reduce response time and permit better coordination and control.

After-hour building security can be provided by good outside lighting, an intrusion alarm system that alerts the appropriate law enforcement office and, if needed, a civilian or uniformed security guard. If these measures are not feasible, it may be possible to arrange for periodic outside checks of the building by state or local police or the sheriff's office.

When a situation causes complete or partial closing of a building to the public, it is important that all tenants receive enough notice and are aware of the procedures to be followed. As noted earlier under "Visitor Control," measures to limit public access will require a court order that is available for public inspection and states the procedures, restrictions and requirements for entry. These measures may mean setting up a search screen operation for the building entrance. If so, requirements for entry should apply to all, with exceptions made only for properly identified law enforcement officers, whom have legitimate business in the building.

Courtroom Security. The courtroom is the focus of high-risk trial activity, and the potential for disruption there is the greatest. Courtroom selection is critical in jurisdictions lacking a room with special security features for high-risk trials. Criteria for selecting a suitable courtroom are include below, and recommended measures within the courtroom include those seen in the Appendices:

- Isolation from public activities and circulation;
- No public access to restricted areas;
- Several means of entry and exit;
- Structural features that serve as barriers and reduce manpower requirements;
- Secure entry and exit for defendants, preferably from a holding cell next to the courtroom; and
- Effective alarm and communications systems.

Defendant Security. One of the most critical and vulnerable points in the custodial process is the time at which defendants are moved between the jail and court. Among the possible incidents that can occur at this time are attempted escapes, assaults on prisoners or security force and self-inflicted injury or suicide efforts. Basic procedures to follow during high-risk trials when moving defendants by vehicle include those indicated below.

- Assign one security officer to remain with each defendant at all times outside the jail/correctional facility or the temporary holding cell.
- Coordinate defendant movement with jail/correctional facility and courthouse staff. All must be aware of the status and location of the defendant.
- Assign escort vehicles in advance and ready guards for the transport vehicle. Survey the route in advance for possible problem areas. Vary routes on a random basis as often as possible to avoid establishing a pattern.

- Maintain constant communications with the base and/or operations center while enroute.
- Use the sally port (guarded entry) system when moving defendant from the transport vehicle into the courthouse. Additional security personnel should be placed around the building entrance, and a trained marksman with a rifle can be on a high vantage point overlooking the entrance and general area.
- Restrain the defendant according to departmental policy at all times except in court, where restraint may be used only under court order.

When not in court, prisoners should be confined to holding cells. Search the cells before placing the prisoners there and again when they leave. Escorting officers should accompany prisoners to their cells and keep them in sight at all times. To ensure alertness, escort officers should be rotated after one or two hours. Defendants should be fed in the holding cell rather than returned to jail/correctional facility. A procedure also should be established for quick removal of a prisoner to the jail/correctional facility in an emergency.

The temporary holding cell should be equipped with toilet facilities. Closed-circuit television and audio equipment can be placed there to let defendants see and hear the proceedings if it is necessary to remove them from court because of disruptive or unruly conduct.

The potential for disruptive incidents in the courtroom can be reduced with careful planning. The search screen process should reduce the possibility of spectators bringing dangerous weapons into the courtroom. The defendant's seat, as well as the witness chair, should be designed to allow the unobtrusive use of restraining devices, if so ordered by the court.¹² An adequate supply of restraint equipment should be available near the courtroom.

All items that could be used as weapons should be kept out of the defendant's reach. Evidence, such as knives, or other potential weapons should be kept out of reach. Ammunition should be removed and kept separate from firearms, and trigger locks should be used. The escort officer should be stationed nearby and to the rear of the defendant to act as a barrier between prisoner and spectator.

Judge's Security. In high-risk trials, threats should receive more critical treatment. However, the degree of security provided for both judges and their families is dictated by the judges' wishes, as well as the nature of the threat.

Judges should receive all available information about threats and should know what security measures are available. A procedure for quick and safe exit from the courtroom and escort to a safe location is advisable. At a minimum, the judges should be escorted from their automobiles to their chambers and when passing through public corridors. While parked, their vehicles should be guarded.

Escort services and/or security officer drivers should be made available during the trials. Chambers should be searched for contraband before a judge arrives each day and at other times, as needed. At the judge's home, security may take the form of outside surveillance or placing security personnel in the house. Local police may provide

periodic checks; however, this should be coordinated by the officer in charge of the detail involved. Temporary alarms also can be installed, but it is important that these and other measures do not unnecessarily disrupt the personal lives of judges and their families.

Jury Security. Threats to the jury may occur in the courthouse, at home or while the jury is sequestered. In and around the courthouse, security can be improved by guards, guarded parking spaces, and escorts to and from the courthouse, the courtroom or in the deliberation room – preferably through nonpublic corridors. In court, the jury is subject to threats from spectators, while at home jurors may be the targets of both threats and actual violence. Judges should immediately learn of any threats to jurors so they can decide whether or not to sequester juries. The prosecutor’s office should be notified of any threats and can decide, along with the judge, whether or not to prosecute individuals responsible for threats.

Sheriffs may think that more security measures are needed than can be provided by their offices. If so, they should ask for help from local law enforcement agencies to ensure adequate protection of jurors and their families. However, additional security measures should be approved by the judge before they are implemented.

Witness Security. Witnesses are often the target of threats. The responsibility for witness security in criminal cases usually rests with the sheriff. During high-risk trials, it may be necessary to provide special protection for witnesses and their families. When extra protection is needed, a court order: will authorize the use of special deputies; will direct the county to pay the costs of that protection; and may protect the sheriff from civil liability for false imprisonment. In many states a *capias* or legal writ is issued to sheriffs directing them to keep witnesses sequestered. For example, some county jails have *capias* sections to house witnesses and other non criminals who are being detained. Witness security may include an escort service, bodyguard (either part-time or round-the clock), or relocation to a temporary residence.

Policy on News Media. Any high-risk trial will generate interest by the media, sometimes resulting in national or international coverage. It is important that a fair and impartial policy be carried out, and all accredited media representatives receive equal consideration. In short, the conduct of security personnel towards media people should be positive, fair and cooperative – within the limits of security planning.

During lengthy trials in particular, security personnel are in daily contact with the media. Some sheriff’s offices recommend “gag orders” from the court prohibiting discussion of the trial or related matters by security personnel. This action channels requests for information to the proper, designated source (such as the sheriff or a public information officer) and protects individual officers from difficult situations.

In large jurisdictions, a court administrator usually handles courtroom admission and the seating of the press. Sometimes the sheriff may be required to make the arrangements. In either case, at least 25-30% of available seating should be reserved for the media. If more media people want admittance than there are seats, then the media should select representatives to be admitted each day. This practice shifts the burden from the authorities and should reduce charges of unfair allocation.

As a courtesy, seats nearest the wall usually are reserved for artists. Moreover, special admittance passes can be issued if necessary. It is best to issue these passes in the

name of an agency, rather than an individual reporter, since agencies may wish to have several different reporters cover the proceedings. Any unclaimed reserved seats should be available to the general public no later than 15 minutes after the proceedings begin.

The courts will usually support recommendations to exclude all photographic and recording equipment from the courtroom or courthouse; to prohibit interviews with defendants inside the courthouse; and to ban all interviews with court officials and the jury. A list of such restrictions should be part of any court order obtained.

Emergency Procedures

This chapter recommends procedures for six types of emergencies: fire, bomb threat, general evacuation, natural disaster, civil disorder and power/utility failure. Many jurisdictions will not need to develop procedures for floods or earthquakes, but if the potential for a particular hazard does exist, a written plan can best guide the staff in its response to the emergency.

Written procedures can increase the chances of saving lives or reducing injuries, and they allow control over potentially disruptive incidents with minimum delay. These plans should not be complex, lengthy or difficult to carry out. If so, they may be self-defeating.

Emergency procedures are only effective when key personnel are fully aware of their responsibilities. Periodic briefings and training sessions conducted by the sheriff's office can ensure understanding of each assignment and procedure. For larger courthouses, it may be necessary to hold briefings and practice evacuations for all building occupants once or twice a year. Proper orientation will help reduce the incidence of panic reaction.

General guidelines for the six emergency plans are in Figure 3-14. Identical recommendations need not be repeated in the individual plans. Rather, some of the basic information should be listed at the beginning of the security manual – for example, emergency phone numbers, personnel and agencies to be notified, people responsible for evacuation and schematic floor plans of the building. Other recommendations will require unique responses based on the particular emergency. For example, during a bomb threat, the security plan for a judge might be evacuation; during a civil disorder the plan might include protection in the judge's chambers.

General recommendations for handling emergency situations include the following:

- Have the sheriff or a designated security officer coordinate all plans, with help from the heads of other agencies in the building.
- Send copies of the emergency plans to the local fire and police departments.
- Set up liaison with local law enforcement agencies to ensure cooperation and coordination during emergency situations.
- Test the response time of the fire department, police agencies and ambulance service.
- Make the same personnel responsible for all building evacuations, rather than having different people handle evacuations during a fire, bomb threat, natural disaster, etc.

In addition to these general guidelines, specific recommendations for the various emergency plans are listed in the next sections.

Fire. The fire emergency plan should also include: (1) instructions on how to report a fire and whom to notify; and (2) a description of primary and alternative alarm methods, such as electrical bell or siren, telephone notice or use of messenger or manually operated alarm in case of power and phone failure.

Have the local fire marshal or department chief review the plan to ensure compliance with local codes. Fire extinguishers and fire-fighting equipment need to be clearly marked and periodically inspected.

Bomb Threat. Bomb threats and actual bombings of courthouses pose serious problems for security officers. Bomb threat procedures should have the following purposes:¹³

- Find the bomb and remove it.
- Identify a hoax and reduce search time.
- Prevent panic and injury.
- Prevent publicity that might cause crank calls.
- Gather information and evidence leading to the identification, arrest and conviction of the perpetrator(s).

The U.S. Department of Homeland Security's Bureau of Alcohol Tobacco Firearms and Explosives (ATF) indicates the need for the following guidelines for dealing with a bomb threat:¹⁴

- Identify all resources available for bomb disposal: local police, fire department, nearby military post or law enforcement agencies.
- Set up a way to handle bomb threat telephone calls. Record information.
- Establish search procedures that identify search teams and their areas of responsibility. See Appendix for an example.
- Decide what to do when a suspicious object is located.

The search is the most important part of any procedure, and searches by trained professionals are the best kind. However, large buildings with few trained professionals available can be searched more quickly by selected volunteers from the building staff. These volunteers have the advantage of familiarity, knowing what items are strange or unusual in their areas. Thus, volunteers need specialized training in search procedures and bomb recognition and should be teamed with a trained security officer whenever possible.

General Evacuation. A partial or total building evacuation may be necessary for reasons other than a fire or bomb threat, such as a gas leak or presence of a noxious chemical. Evacuation plans should follow the guidelines in Figure 3-14.

¹³ California Office of Emergency Services, *Bomb Threats* (Sacramento, California, 1971).

¹⁴ U.S. Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, *Bomb Threats and Search Techniques* (Washington, D.C.: U.S. Government Printing Office, 1974), p. 6-7.

Natural Disaster. Many areas are particularly prone to earthquake, flood or forest and brush fire. Plans for such disasters should concentrate on lifesaving aspects. Court security personnel are also responsible for the safety of judges and court staff, safeguarding and retaining custody of prisoners, and protecting records and evidence in certain circumstances.

Disaster plans should include (1) the location and availability of resources, such as heavy equipment and manpower to aid rescue efforts in the event of major structural damage, and (2) alternate means of communication, usually a radio with a self-contained power source. The plan should describe the frequencies or channels used and should identify the agencies on that channel.

In many jurisdictions, the likelihood of disasters is remote, and elaborate planning is not required. In these cases, elements of other existing emergency procedures will cover most situations.

Civil Disorder. There are two general types of disorder. In both, coordination with other law enforcement agencies is vital. First are disorders of a serious, long-term nature. These are general in scope, with widespread disturbances and possible curfews. Second are disorders that may have high levels of violence, but the incidents are of short duration and usually occur only during business hours.

During the first type of disorder, all nonessential services are suspended. The courts will usually remain open only to process demonstrators, looters and others associated with the disorder. The second type of disorder may involve large groups of demonstrators who try to disrupt the judicial process through militant actions, to the point of trying to enter the courthouse. A sheriff's response to this situation is complicated by large numbers of people within the courthouse.

Civil disturbance procedures should include the following:

- Plans to secure or control all entrances and windows providing access to the courthouse;
- Policies on who is authorized to issue and use supplemental weapons, such as shotguns, tear gas and rifles;
- Policies on safeguarding prisoners and protecting vehicles;
- Mobilization plans for additional manpower;
- Feeding, relief and housing procedures in case of a prolonged demonstration;
- Arrest procedures, including an operations plan and documentation procedures; and
- Policy for use of photography (both still and movie) for record keeping.

Power/Utility Failure. In most cases, a power or utility failure is more an inconvenience than a true emergency. Some panic can develop in windowless courtrooms without emergency lighting, and people trapped in elevators need immediate attention and reassurance. In addition, some electric locks will need to be unlocked by hand.

A power or utility failure plan should include: (1) a list of the day and night emergency service numbers of all utilities and building engineer personnel; (2) the locations of all main electrical panels and cutoff points for gas, water, electricity, phones

and steam; and (3) emergency lighting for courts in session, key offices, temporary holding areas and other designated locations.

Postevent Review of High-Risk Trials and Emergencies

As in hostage situations, a post-event review is important here too. If this review produces candid, constructive criticism, management can assess the value of existing procedures for special situations. The purpose of any review is to improve the quality of operations by ensuring concerned parties know what was done properly and what was not. Suggested guidelines for conducting a review follow.

1. Hold a meeting of key personnel as soon as possible after an incident occurs. The officer in charge should describe the incident, and the procedures used to control it. This meeting is necessary because all participants may not be aware of what happened outside their own areas of responsibility.
2. Evaluate each procedure used during the incident in terms of its suitability for accomplishing its purpose. The need for procedural change can be identified here.
3. Evaluate individual performances in carrying out assigned tasks in a professional manner, being careful not to “talk down” to anyone. Offer positive steps for improvement.
4. Briefly summarize the review findings.
5. Prepare a detailed report of the incident, problems encountered and steps taken to overcome them, with recommendations for improved planning and procedures.
6. Revise the security plan, using the report as a basis.

COURT OFFICER’S MANUAL

This section discusses a recommended format and contents for preparing a court officer’s manual. The information here is a combination of similar manuals developed and used by sheriff’s offices. The format and outline apply equally to court-appointed court officers and deputy sheriffs assigned as court officers.

Officers responsible for writing or revising a court officers’ manual should use the contents section as a guide, which they can change to fit individual circumstances. In jurisdictions with much courtroom activity – in terms of both caseloads and the number of courtrooms – the manual may be a major document exceeding 100 pages. In jurisdictions with limited activity, the book may be much smaller and could even be incorporated into an overall security procedures manual. This is especially true if the larger document spells out court officer’s duties in particular cases, such as the manual described in the previous section of this chapter.

Purpose and Design

A court officer’s manual provides clear, concise information and guidance. It is basically a “how to” document and describes many actions taken during the court

process. The manual helps people who do not perform these duties on a full-time basis, and is a ready reference for resolving the problems that may arise in daily activities.

As noted before in this chapter, improper conduct by a court officer has often been used successfully as the basis of a motion for mistrial or reversal in the appellate courts. Such incidents can be reduced if the court officer can study and refer to comprehensive written instructions.

A well-prepared manual will do the following:

- Describe a court officer's duties and responsibilities;
- Provide a source of information and reference that helps court officers better understand their role as court officers;
- Give basic background information on the legal and organizational framework within which the court officer operates; and
- Explain general procedures for courtroom and building security.

Court officers' manuals from different areas of the United States show no set format; rather, each has evolved to suit local circumstances. Although many court officers' manuals are permanently bound, the use of a looseleaf or similar temporary binder should be considered. This format allows easy addition, removal or change without the expense of a new printing, thus keeping the manual current. Detailed suggestions for manual design are included under the earlier section on the procedures manual.

Contents

The first step is to prepare a topical outline, following the model shown in the Appendix as a general guide. Substitutions and deletions can be made freely, as needed. The topical outline should have enough detail so that the user can easily find a particular section of immediate interest. The following discussion is a partial listing of subjects to include in the manual.

State Judicial System. As officers of the court, court officers should be generally familiar with the structure of the state judicial system. It is not necessary for them to memorize details, but pertinent data should be available for reference in the manual. This section also should have a good description of the state jury system. However, in describing the state judicial system, the manual's authors should consult the district attorney to ensure completeness and accuracy.

Legal Requirements. In most states, legal requirements cover court responsibility for sheriffs or court-appointed officers. These requirements should be cited and quoted. Matters involving quotes of state statutes, state or U.S. court decisions or anything with legal implications should be reviewed by a lawyer for accuracy and completeness. State codes are subject to periodic revision, and the manual should say that all codes cited were in effect when a manual was written or revised.

Organizational Structure and Responsibilities. If the size of a department warrants, the organization of the major division under which the court officer's service falls should be shown. For each subdivision, prepare a diagram showing the rank and responsibilities

of the unit commander and list those under each commander. For smaller departments, a detailed breakdown may not be necessary.

Court Officer's Duties. A court officer's work can be described as both clerical and security related. The first duty may include preparing various forms and keeping records on defendants and court activities. The scope of these duties should be clearly defined in writing. The court officer must not be overburdened with clerical duties that are more appropriate for other court staff. Otherwise, a court officer's effectiveness in security-related responsibilities is reduced. Of course, this view does not apply to those court-appointed court officers who may have minimal security tasks.

The court officer may have primary court security responsibility or may share it with a security officer. These duties should be clearly defined in writing. They will vary among jurisdictions, but a typical list of duties would include the following.

- Court officers should promptly and properly obey all lawful orders and directions of the court.
- Court officers should maintain order in the courtroom to make sure that litigants, attorneys, court staff and spectators conduct themselves properly.
- Court officers should cooperate with the court clerk and staff to assure that court proceedings run smoothly.
- Court officers must be alert and ready at all times to control unusual or unexpected situations in the courtroom.
- If they are law enforcement officers, court officers are not limited to courtroom duties. They also must be alert to violations of law outside the court.
- Court officers should be informative and courteous but, as noted before, they should not attempt to give legal advice or discuss the relative merits of a case. Such action might jeopardize or influence the results.
- Court officers should promptly submit all required reports and forms and relay any unusually circumstances or information to supervisors for evaluation and action.

The court officer's manual also could cover special considerations, such as responsibility for jury security and care, how to handle incustody defendants and the problems presented by situations, such as juvenile hearings or hearings on mental competency. These and other special circumstances are discussed in detail under the procedures many section of this chapter. However, each locality must decide whether those topics are more suited to the court officer's manual or the security procedures manual.

A final point on content: For the sake of clarity and accuracy, all abbreviations used in the manual should be listed in a glossary. For example, CCP = Code of Civil Procedures, GC = Government Code and PC = Penal Code, etc.

CONCLUSION

The goal of an effective court security operation is to establish appropriate protective responses for all persons who are using the building and are part of the judicial

process. To achieve this goal, it is important to have clear written policies and procedures. This chapter has provided general information and guidelines for developing both.

The major recommendation in this chapter is that each jurisdiction prepare or update both an overall security procedures manual and instructions for court officers. The latter can be either a separate documents or part of the broader manual, but both guides are necessary for a truly effective court security operation.

Chapter 4

PHYSICAL SECURITY

Physical security is only one aspect of a total security program and usually has three elements: building structure; hardware or personnel used against intruders; and fire protection and safety. Physical security can be defined as a system of barriers designed to (1) *detect* intruders within protected areas and inform security forces of the intruders' presence, (2) either *delay* the arrival of intruders at their targets or *prevent* them from taking any action, and (3) *deter* potential intrusion. "System" is a key word in this definition -- the systems approach to security requires policies and procedures work together to achieve a unified effort.

This chapter examines certain aspects of physical security, and how it fits into an overall court security plan. Architecture, equipment, security procedures, and personnel are discussed only briefly, since each is covered in a separate chapter. Rather, this chapter focuses on physical security surveys and how to conduct them. Using the methods outlined in this chapter, sheriffs can do a comprehensive security survey in any courthouse.

PHYSICAL SECURITY BARRIERS

Physical security involves setting up such barriers as fences, locks, gates, vaults, alarm systems, sensory devices and lighting, in addition to using guards, watchmen and dogs. Barriers define the physical limits of an area and prevent entry. They should be considered the "time delay" part of a security program because they make entry into a building or area more difficult and, thus, more time consuming.¹⁵

This chapter discusses physical security barriers in these five general categories:

1. Natural
2. Structural
3. Electrical or energy
4. Human
5. Animal

Natural barriers include rivers, cliffs, mountains, ravines, steep grades and similar topographical conditions. An architect can sometimes take advantage of these natural features, but a determined intruder usually can overcome these barriers easily. Thus, natural barriers are often more effective when used with one or more of the other types of barrier.

Structural barriers are man-made and usually include fences, walls, doors, gates, grilles and windows. These barriers control entry into a building and key areas inside it.

Electrical or energy barriers include lights, sensory devices, alarms, closed-circuit television and electrically operated communications systems.

¹⁵ Richard Post and Arthur A. Kingsbury, *Security Administration: An Introduction*, 3rd ed. (Springfield, Ill.: Charles C. Thomas, 1977), p. 478.

Human barriers, the core of any physical security system, include law enforcement officers, guards and watchman.

As **animal barriers**, dogs have been used widely in law enforcement and security work. They can be patrol animals accompanying the handler and acting only on command. In addition, they might be trained to act independently within a building or an enclosed area, such as a storage yard. When used without a handler, dogs can learn to attack any intruder on sight. Note that dogs must be used regularly and also retrained as needed, so they will keep their specialized skills. Their use in court security has been limited to search situations involving persons and explosives. On occasion, horses are also useful to augment control of demonstrations outside a courthouse or any other public areas.

PHYSICAL SECURITY IN COURTS TODAY

A court security program is somewhat different from industrial or governmental security programs, where one must protect both a building and sensitive or classified information, with the latter perhaps requiring security clearances for certain personnel. For example, court and county records, unless sealed by court order, are in the public domain. Moreover, the employees who handle those records are hired under a state or county civil service program or a merit program and seldom have thorough background checks. Some large sheriffs' offices, where increasing stress is placed on the officer, may use background checks and even psychological evaluations in personnel selection. However, in smaller jurisdictions, employment may be based on personal knowledge of the person applying, and sheriffs' officers usually have no formal background investigation programs.

Whatever the differences in security programs, in the last several years, violence directed at public institutions, including courthouses, has shown the need for protective security systems. However, those systems should not interfere with the activities of the institutions it protects. Therefore, as noted elsewhere in this manual, the security planner must set up a system that strikes a balance between physical security and building operations.

Court security can be improved by simple physical changes for reasonable costs. Some ideas for inexpensive security improvements include items such as external lights, quality locks and hardware on doors and windows, intrusion alarms and duress alarms and emergency lighting in the courtroom.

Many jurisdictions have recognized court security requirements and have taken effective steps to meet those needs. On the other hand, some people have viewed sophisticated equipment as a single answer to most security problems. Actually, a balanced mix of architecture, manpower and equipment is necessary, as discussed in the following sections.

Architecture

The most cost-effective way to improve overall security is to incorporate security features in the design of a courthouse. Courthouses built before the mid-1970s show few, if any, security considerations, but incidents of the late 1960s and early 1970s caused a major shift in thinking, and renovations became necessary. Older courthouses were

modified, with all but the necessary entrances closed and entry to judges' chambers restricted. For a brief period, overreaction caused large sums of money to be spent hastily and sometimes unwisely. For example, one western courthouse is reported to have spent \$700,000 to change one courtroom for a high-risk trial. In some cases, funds appropriated for a certain year had to be spent or lost; this situation resulted in an emphasis on spending, rather than getting the best value.

Many architects designing courthouses today are concerned with security. Better prisoner circulation is being planned, public circulation is more clearly defined and restricted or controlled areas are isolated in increase security for judges, staff and jurors. However, despite the new security awareness, many unnecessary and costly mistakes are still being made and must be corrected after construction (see Chapter 7). For example, even some of the newer courthouses do not have witness waiting rooms, where witnesses are separated from possible encounters with prisoners or their relatives and friends.

Manpower Impact

Personnel are the key to a physical security program for courts. They guard buildings and some occupants, operate or monitor equipment, apprehend intruders and respond to any security problems within a building. However, court violence in recent years showed that security personnel often were not able to cope with such situations. For example, many security officers and court officers were older and not physically or psychologically prepared to deal with violence.

This problem was solved through personnel selection and training. First, younger, more agile men were assigned to courts where incidents were likely. Also, there was emphasis on selecting officers who were psychologically prepared and had shown sound judgment and self-control in times of stress. Second, there was greater emphasis on specialized training to help officers deal with a variety of incidents. This training focused on such areas as civil disturbance control, dealing with disturbed persons, bomb threats and high-risk trial procedures, special weapons training, first aid and cardiopulmonary resuscitation (CPR).

Equipment

With the increased security awareness in recent years, many new developments have occurred in the equipment field. Following is a list of equipment most likely to be used for protecting courthouses and courtrooms. Chapter 5 discusses these items in greater detail.

- Perimeter and exterior building lights to help deter and detect intruders (note that lighting is more valuable if combined with periodic inspection or patrol of an area);
- Door and window locks and improved electrical and mechanical lock systems;
- Alarm systems to protect a building at night or serve the courtroom in emergencies;
- Closed-circuit television (CCTV) to monitor large spaces with limited personnel;

- Magnetometers (metal detectors) available in three basic models: portable walk-through, hand-held and units permanently installed in courtroom door frames; and
- Cameras to photograph spectators before they are admitted to high-risk trials (part of a search screen operation).

Ideas about Physical Security

The lack of unified opinions on physical security makes the security planner's job more difficult. The planner must deal with the different views of judges, prosecutors, defense lawyers, court administrators and interested groups in the general public when creating and attempting to garner support for a revised or continued security plan.

Judges are particularly conscious of the need to protect the individual rights of all involved in the trial process. Thus, they may not support all of the security planner's recommendations. Prosecutors generally have a similar view; however, when directly threatened, both groups may want the strongest possible security measures taken. Defense attorneys usually object to many physical security measures, which they believe create a bad image for their clients, and, thus, prejudices their cases. The general public tends to accept "reasonable" measures with few complaints, while some groups strongly oppose certain measures.

Within each group, there are often differences of opinion. For example, judges, who have been exposed directly or indirectly to court-related violence, are more receptive to physical security measures than those having never come in contact with such violence. Some judges in the first group may actually prefer to be armed when on the bench. The fact of the matter is each group has an opinion, and the more involvement the planner receives in the early planning stages usually positively correlates to greater support and acceptance. The most efficient method for soliciting this type of information, in most cases, is through surveys.

THE PHYSICAL SECURITY SURVEY

The survey is a critical onsite examination and analysis of the court building. It determines the present security status, identifies a lack or excess of security, determines what protection is needed and recommends ways to improve the situation.¹⁶ Two key factors in any physical security or crime prevention survey are identifying risks or opportunities for crime and recommending ways to address any weaknesses.¹⁷ A comprehensive physical security survey will provide the facts needed to develop a good security plan.

The following information will give the security planner some basic ideas on how to conduct physical security surveys. Note, however, any survey must be designed to fit individual circumstances, and these suggestions may have to be adjusted to particular needs.

¹⁶ Raymond M. Momboisse, *Industrial Security for Strikes, Riots and Disasters* (Springfield, Ill.: Charles C. Thomas, 1968), p. 13.

¹⁷ Arthur A. Kingsbury, *Introduction to Security and Crime Prevention Surveys* (Springfield, Ill.: Charles C. Thomas, 1973), p. 6.

Survey Elements

A comprehensive physical security survey takes into account all aspects of a building and its nearby grounds, including both internal and external spaces, structural features, equipment and the activities of building occupants.

Structure

This includes all outside and inside building elements – *e.g.*, lighting, doors, windows, entrances, hallways, stairways, offices, courtrooms, service areas, temporary holding cells, safes, vaults and records storage areas. The survey should include all spaces, including both public and restricted or controlled areas, regardless of their tenants.

Equipment

The availability and use of equipment is a key aspect of physical security. Different types of equipment available for courthouse use are discussed in Chapter 5. A survey should identify the types of equipment used, its effectiveness and possible equipment needs.

Perimeter

Areas near the court building that may influence security, including parking spaces, public parks around the courthouse (often found in smaller communities), fences, gates and lighting.

Noncourt Tenants

When a courthouse is also occupied by noncourt agencies, it is better to conduct a comprehensive, building-wide survey rather than one limited to court areas. Many jurisdictions limit the study to courts and its related functions, but this could cause serious gaps in overall building security. The needs of all occupants can best be met by including them all in the survey. It is important to convince noncourt agencies of the benefits of participating, and that the security survey can perform a needed service at minimal cost by identifying weaknesses and potential problems. Tenants with a strong internal security operation should participate through a joint venture arrangement, for example, as its special skills may contribute significantly to the overall study.

Work Schedules

Survey personnel should be thoroughly acquainted with the normal operating hours of all building occupants. Also important are the hours for closing all or part of a certain floor or the entire building, weekend operations and any special considerations, such as use of building space for civic functions.

Survey Activities

The survey's success depends largely on how complete basic presurvey activities are. To build a good foundation for the study, security planners should take the following actions.

Prepare a Needs Statement

There may be many reasons for conducting a survey. For example, such an effort may never have been done before and is needed to revise the current security plan. Or a previous study may be obsolete because of later structural or procedural changes. In addition, there may be recent incidents or evidence of serious deficiencies to consider, and a survey could point out ways to correct those problems.

Describe Survey Goals and Objectives

The goals statement should be general. For example, “to improve overall physical security by identifying specific areas needing attention and by recommending necessary courses of action” is a broad goal.

The objectives statements identify specific actions to meet survey goals. Objectives must be realistic (*i.e.*, based on an assessment of actual security needs) and within the limits of funding and manpower levels set by legislative authority. Objectives may include increasing security for the courtrooms, judges and juror; defining circulation patterns for prisoners, court officials and the public; reducing thefts; developing a comprehensive alarm system; improving emergency response time; upgrading the system by purchasing equipment; and improving temporary detention facilities. The objectives are the steps, which once successfully completed, allow the goal(s) to be achieved.

Identify Authorizing Agency or Individual and Determine Responsibility for Carrying Out Recommendations

The survey may have been authorized by the presiding judge, sheriff, court administrator or board of supervisors, and one of those authorities may have to carry out survey recommendations. There should be a clear intent to act on those recommendations, which may mean spending money and/or making manpower adjustments.

Those requesting the study should understand that costs for implementing recommendations should be included in a regular budget or a special appropriation request. Similarly, the agency carrying out survey recommendations needs a thorough understanding of the budget process, as well as any fiscal limits affecting implementation. For example, funds may be needed for more than one year.

Select the Team

The best qualified people available should be on the survey team. The group should include persons with specialized skills (*e.g.*, in communications or alarms) and those with experience in managing and conducting security programs. Technical knowledge in court security methods and special community requirements would be desirable, and previous survey experience is helpful, but not required. Team members may be drawn from other government agencies or private consultants.

The individuals selected need sound judgment and reasoning, should speak well and communicate effectively with others and should be good writers. They need to be mature enough to deal with judges, court administrators and senior members of tenant agencies. In addition, they often will need tact and diplomacy to overcome resistance and gain cooperation.

Develop a Format

Physical security experts have tried to develop a single model survey format, and have concluded this is not possible. No two surveys are the same, and the willingness to try new approaches is important. Basic elements are common to every comprehensive survey, but each one develops from the unique circumstances of the building involved.

As a first step in developing a survey format, the survey team should prepare a list of major areas of concern. The procedural areas can be identified by reviewing a security procedures manual, if one exists. This division offers an orderly source of information for presenting findings, conclusions and recommendations, and will make the survey report easier to write.

For each area, security or security-related questions should be worded so the response can be a simple “yes” or “no;” although, sometimes a narrative response may be more appropriate. Good surveys will require both kinds of questions. Usually, the question “why” does not need to be asked after a “no” response. For example, a negative answer to the question: “Are functioning locks provided for all doors to the courtroom?” does not require further explanation. The purpose of the survey is to offer recommendations, not to explain why the locks are not there. In this example, the recommendation might be to purchase six key-operated, dead-bolt, cylinder locks for the courtroom doors at an estimate cost of \$12.

When developing a security questionnaire, there is no set order for listing the questions; whatever works best should be used. For example, going from general subjects to specific ones is a possible approach. At any rate, the format used should make it easy to divide responsibility among the surveyors. Finally, the survey questionnaire format should provide a clear, simple picture of conditions, and any detailed notes taken during the survey will add to the picture.

Gather Data

Much information about a building is already available and can be gathered by the team before the actual survey. Such information may include the following:

- Previous survey reports or studies;
- Floor plans from the building’s engineers, manager or architect;
- Inventory of all security equipment;
- Incident reports from sheriffs or other local law enforcement or peace officers;
- Operating regulations for the building;
- Traffic volume (number of visitors, defendants, etc.) and number of trials (jury, nonjury);
- Security or operating procedures established by the sheriff or building tenants; or
- The community’s fire code.

This represents the survey’s initial database. Previous surveys or studies are particularly important, since they should reveal prior security problems and recommendations. At this time, or as the survey goes on, it is possible to find out how many previous recommendations were implemented or even why certain ones were not. This information is important to the current survey because it may identify obstacles otherwise are not readily apparent.

Meet with Department Heads of Tenant Agencies

No matter what the purpose, surveys often meet with suspicion and resistance, which are usually overcome by laying the proper groundwork. This can be done through a meeting of the sheriff and survey team members with all concerned tenant managers to explain the survey, answer all questions, and ask for their cooperation and any ideas about security risks and possible solutions. This meeting, to be held when the survey team is ready to begin, should identify who requested and authorized the effort; introduce survey team members and cite their special skills; and explain how the survey will work. Tenants also should be told when to expect the team to visit their offices.

During the meeting, tenants should be asked to cooperate by providing information about their operations. This may include copies of operating orders and a statement of what their offices do, the number of personnel and daily visitor, special security problems (*e.g.*, involving records or money), and any other data needed to complete the survey. This information should be gathered before any onsite visit(s).

The tenants should be informed more meetings will be held after the draft findings and recommendations are completed, to ensure accuracy and provide an opportunity to discuss matters individually before final recommendations are made. This point often assures the tenants the survey is meant to help them too. Based on this meeting, the team should try to assess the attitudes and willingness of individual department and agency heads to implement change.

Conduct the Survey

Two or more people should conduct the survey whenever possible. This encourages the use of specialized skills in evaluating specific areas – *e.g.*, fire, safety and prevention, communications and alarms. Teamwork also reduces the time needed to conduct the survey, evaluate findings, develop recommendations and prepare the final report. The team concept helps stimulate thoughts and ideas, allowing professionals to discuss ideas with one another, which often results in better recommendations.

It is important to have a system which allows the most complete collection of information. A small building may be surveyed by a two-person team, while larger buildings may require more people. The number needed to conduct the survey will be determined by the scope and depth of the effort.

Along with the questionnaire, other aspects of the survey are personal observations, interviews, and gathering documents not previously collected. In large, multistory buildings, it is usually better to conduct the survey floor by floor. This may seem repetitious, but the procedure usually gives a clearer understanding of findings and recommendations and offers a logical separation by tenant areas. The equipment inventory should be verified at this time.

All notes and questionnaires should be saved as part of the permanent record and as reference material. These data should be combined with information collected in the presurvey activities; and the combined materials will be the basis for the report.

Survey Report

The report can be the most important, evidentiary part of the survey. It is a permanent record of findings, conclusions and recommendations and may include an implementation plan. The report gives management a clear understanding of current

security conditions and what changes are needed. It provides a basis for improving security through additional manpower, training, equipment, and through changes in structure and procedures.

Format

This is a matter of preference, and there are many acceptable styles. However, remember the value of a report is lessened if it is not clear, concise, easy to read and well organized.

Contents

There are three (3) major areas of the survey report – background, summary of finds, conclusions and recommendations; and detailed findings, conclusions and recommendations. The **background** section provides information gathered before the survey, including the following:

- The requesting authority and purpose of the survey (discussed earlier under **Survey Activities** in this chapter);
- Members of the survey team (include parent agency and a brief summary of experience and technical specialties);
- Dates the survey was started and completed;
- Previous surveys and studies and an assessment of future security threats. This assessment helps define security problems and can be based on (1) past trial experience, including common factors in trials; (2) data, such as population density, distribution, ethnic breakdown and economic status; and (3) potential for criminal acts, such as burglary and for natural or man-made disasters common to the area;
- A brief description of the facility, including outside grounds, type of building construction, age, number of floors, approximate square footage and any other significant descriptions (details should be included later in the report);
- Tenant agencies and the number of employees working in the facility. If the number of agencies is small, staff members can be listed by title. If there are many agencies in the building, it may be better to list them in an appendix;
- The agency responsible for courthouse and courtroom security (describe security provided for both working and nonworking hours); and
- Summary of security incidents in the building during the past five or more years. If many incidents occurred, this information may be more appropriately included in an appendix.

The **summary of findings and conclusions** should be presented in one or two paragraphs, and the **summary of recommendations** should briefly list major points. Examples of the latter: “Window and door hardware and locks on the first floor should be replaced (estimated cost \$700)” or “additional equipment for court security should be provided (estimated cost \$4,500).” Funding implications for the agencies concerned should be listed in appendices, with a breakdown by agency of costs for manpower, training, equipment and structural change.

The presentation of **detailed findings, conclusions and recommendations** depends on the size and structure of the courthouse. For multistory buildings, it may be best to present details floor by floor or by functional groups (*i.e.*, those with similar activities). Recommendations can be grouped together at the end of the narrative or presented throughout the text, but should always be specific and easy to understand, with alternative courses of action suggested whenever possible. All recommendations should be numbered in sequence.

Any supplemental material should be included in **appendices** to reduce the volume of the main text. Appendices may include office sketches (architects' floor plans are not necessary), statistical data and inventories. However, caution should be exercised when attaching this information, especially if the materials could be accessed by anyone not originally intended.

Draft Report

The team should use all the data gathered to draft the findings and conclusions. Then they should review this section carefully for accuracy, and obtain any additional data needed. Team members can use the findings and conclusions as a basis for developing recommendations, including various alternatives. In recommending equipment, they should not specify brand names, and should remember that certain security devices, such as doors and locks, must be approved by the local fire marshal. Surveyors should give both complete cost estimates and personnel data when training programs are suggested. Structural recommendations should include time and cost factors and any anticipated interference with normal building operations. Finally, a plan for implementing the recommendations can be included with the draft.

When the draft report is ready, the team should have individual conferences with the officers and tenants responsible for different procedures or areas. This allows those groups to express different opinions, clarify points and correct errors. Offering managers the opportunity to review recommendations on their activities before the final report is written is a matter of courtesy and good management. It may also prevent minor errors of fact or interpretation which could adversely affect acceptance of the overall report. Moreover, many managers will start implementing the recommendations based on this review, a fact that can be noted in the final report. When these conferences are completed, the final report should be written.

Final Report

The team should notify the requesting agency or individual when the report is complete. All key personnel responsible for carrying out recommendations should be invited to an oral presentation of the final report by the team members. Some departments give advance copies of the report to persons attending this meeting, while others prefer to distribute the report after the presentation; this is a matter of individual or agency preference. At the presentation, survey team members should be prepared to defend their ideas with facts and must be familiar with the results and impact of each recommendation on both the security program and daily building operations.

Postsurvey Activities

Carrying Out Recommendations

Usually, all managers in a surveyed building will be asked to review security recommendations affecting operations, and to indicate, preferably in writing, which ones they are prepared to implement. The managers should give written explanations for those not being carried out. However, remember only departments of the requesting authority or the sheriff's office can be *required* to prepare implementation plans. Other tenants can only be *encouraged* to do so, and their actions may need approval from parent organizations. The process may be guided or assisted by Judicial Orders Specifying certain rules, etc.

Implementation plans should state basic objectives and resources (*e.g.*, manpower, money, time, professional services, space), though the plans need not be highly detailed. Especially helpful is a work plan, in the form of a chart showing dates to start and complete major activities. If a department lacks the skill to prepare this plan, it should seek help from the county planning officer.

Follow-up Inspection

Finally, many excellent surveys have had little effect because there was no follow-up review of the actions taken to carry out recommendations. The requesting authority should be urged to require periodic inspections and reports on whether actions have begun. Later, it will be important to develop an ongoing monitoring system to evaluate the effects of those actions.

Chapter 5

EQUIPMENT

Equipment is an important part of court security. It may include electronic or mechanical devices, such as a basic intrusion alarm system or walk-through or hand-held magnetometers, as well as more sophisticated items such as microwave alarms, closed-circuit television (CCTV), or infrared viewing and photography devices. However, equipment alone is not the solution to a security problem; at best, it is a supportive tool when used by trained personnel in a well-prepared plan or procedure.

This chapter gives guidance on what equipment is needed and standards for choosing the right items. The chapter also suggests ways to improve procurement procedures, and discusses various types of equipment used for court security.

BACKGROUND

State of the Art

During the past few years, rapid advances have occurred in all fields of technology, especially in specialized security equipment. Miniaturized computer circuitry have made possible devices considered science fiction only a few years ago, such as: intrusion detection systems, night viewing devices using amplified star light, and individual transceivers (transmitter-receivers) and weapons that easily fit into a pocket or can be hidden in even smaller areas.

However, the state of the art is constantly changing and should always be evaluated, since most items have built-in obsolescence. Developments are so rapid by the time one idea is put into production, a new and improved one is underway.

Key Planning Issues

Planners must consider many factors before installing a protection system. To prevent serious budget problems, planners should evaluate needs, cost effectiveness, and manpower requirements. A security systems expert can design a secure, sophisticated protection system using the latest developments in alarms, CCTV, sensor devices and physical barriers. However, it does not make sense to have a \$25,000 system guarding \$2,000 - \$3,000 worth of assets.

In addition, image building should never be the main reason for getting equipment. For example, buying an expensive X-ray screening device to impress others can backfire when the unit rarely is ever used. This kind of waste could affect future efforts to get approval and funds for essential equipment, especially high-cost items such as CCTV and sophisticated electronic systems.

Equipment is seldom a complete substitute for manpower. For instance, alarm systems require a security force response, and a CCTV camera is of little value if no one is available to monitor it and respond when necessary. More equipment often means a reduction in manpower, but cost comparisons should be made first.

To determine the cost effectiveness of a piece of equipment, compare the total estimated costs for both equipment and people performing the same function. Note manpower costs are involved in both estimates, since personnel are needed to monitor

and operate equipment and respond to an emergency situation. When the two total estimated costs are computed over the expected lifetime of the equipment (perhaps 10 years), one can determine which solution will cost less and/or is justifiable.

To summarize, major equipment purchases should be part of a thorough and well-documented budget plan. Required manpower estimates should be in line with equipment procurement projections to keep the security department from having too much equipment and not enough manpower to use it properly or vice versa.

Finally, all equipment and supplies issued to a department should be recorded in a proper accountability record system, which will be the basis for inventories and audits. Records should be kept of all requisitions, purchases, deliveries and related correspondence. Good records will provide a supervisor with readily available information on quantities in stock, what has been issued to whom and what needs to be reordered.

EQUIPMENT SELECTION STANDARDS

To select the best equipment at the lowest cost, security planners should follow certain standards or guidelines.

Need

The need for equipment may be apparent after a security survey or change in operating procedures. The determination can be made independently or with the aid of a security equipment expert, who often can help prevent needless expenditure(s). The need should be clear and easy to explain, so the right equipment can be matched to the most appropriate need. This is important to assure the purchase of an effective item does not have costly, extra features.

Suitability and Performance

Performance specifications should be drafted from the needs statement. These detailed requirements will define what a piece of equipment is expected to do and will help determine the best kind of equipment to buy. Performance specifications are discussed in more detail later in this chapter in the **Guide to Procurement Procedures**.

Matching the performance specifications against a technical data sheet for the item being considered should determine whether the equipment can do the job needed. This review will also alert planners to sales agents who may be selling them unnecessary items or features.

Reliability, Obsolescence and Availability

The items purchased should have proven reliability. Ask other buyers about their experiences. A new product may have unexpected “bugs,” which show up after purchase and installation, and may mean excessive maintenance. A courthouse cannot afford to be the test site for those new items.

Items purchased should be within the state of the art and not currently or nearly obsolete. Bargain prices are often offered for items going out of production or being

substantially changed in design. Such items seem like bargains but may become useless in the long run because service and parts are unavailable.

If possible, limit procurement to a product offered as a standard shelf item and available within a reasonable time. Some items have such a limited demand that they are only manufactured by special order, which can greatly delay installation.

Design Limitations

All electromechanical equipment has built-in design limits. These should be identified before purchase and a judgment should be made as to whether the limitations will keep the devices from doing a job well. For example, to function properly, much electronic equipment needs a constant power supply without fluctuating voltage. Interruptions in power or voltage changes can cause incorrect instrument readings or other malfunctions. Also, most tear gas canisters are easily affected by extreme temperature and humidity, and magnetometers may locate metallic weapons but not such objects as plastic or wooden knives and letter openers.

Compatibility

Compatibility with existing equipment is a prime consideration for new purchases. For example, all communications equipment should be on a common frequency or capable of being linked by a repeater unit. If separate frequencies are required, there should be a point where the various units can be monitored and coordinated.

Compatibility reduces inventory requirements for items such as portable lights, desk lamps, battery-operated equipment, cameras and office machines using expendable supplies. Some agencies tie up large sums of money by stocking different types of spare parts and other inventory items because the equipment is not similar.

Cost

The cost of an item should be calculated through a formula. Note that the most cost-effective item often has a higher initial cost. For example, key-operated door locks with replaceable cylinders are more expensive but also more practical than locks which must be replaced entirely in order to change keys.

Manpower Impact

Most major pieces of equipment have manpower requirement, which must be considered before purchase. For instance, walk-through magnetometers require at least three operators (two men and a woman) so that both men and women can be searched when something suspicious appears. In addition, CCTV must be monitored constantly, although grouping all monitoring jobs (for alarms, CCTV, etc.) at one location can reduce personnel needs.

Equipment also should be examined in terms of its ease of operation and maintenance, and any training that might be needed. Sophisticated equipment, such as mobile laboratories, may require either specially trained and skilled laboratory technicians or maintenance personnel for proper use. Many sheriffs' offices provide at least routine maintenance of vehicles, weapons, radios and alarm equipment. Unless this

is done by civilian staff, it takes sworn officers away from their primary law enforcement duties.

Space Needs

Both operating and storage space are important. For example, adequate and secure space must be available for the terminal points of CCTV and alarm systems. In addition, there must be space to store and protect equipment that is not being used. Bulky items not in constant use should be kept near the place of use if possible. Similarly, walk-through magnetometers and other items used in a search screen should be stored where readily available.

If space is not available in the courthouse, it may be necessary to store certain equipment elsewhere. In this case, the additional factors of transportation and time must be considered.

Installation and Maintenance

The ease and cost of installation should be factors in equipment selection. A special installation team means more expense, and long delays may occur if there is an installation waiting list for the equipment. Check the backlog of installations and decide whether the waiting period is acceptable.

Select equipment which does not need frequent servicing. Ask current users of the equipment how often service is required, and how long it takes. New equipment almost always requires some servicing, but long-term maintenance needs can be reduced. Avoid items that may need frequent maintenance because of faulty engineering or sensitivity to heat, cold or shock, or those that are easily damaged by unskilled operation.

Service should be readily available, and done locally if possible, especially for routine maintenance. More complex and regular service may require a service contract. Many national companies provide service for several states. This type of coverage increases the service costs and the possibility of excessive delays, both of which have a negative effect on security programs.

The service company should have enough spare parts. A good company can accurately estimate the failure rate of components in the equipment it services and will usually maintain an adequate inventory of spare parts. However, some firms try to save money by getting spares from a main supplier; this nearly always results in delay. Moreover, foreign products may involve ordering parts from another country which could cause months of waiting.

GUIDE TO PROCUREMENT PROCEDURES

A county purchasing authority usually buys equipment; only rarely is a sheriff authorized to make direct purchases. Complaints that the purchasing agent did not buy what was needed are sometimes heard as excuses for faulty or inadequate equipment. However, a close look usually reveals a breakdown in communications between the sheriff and the purchasing agent. This problem can be overcome with a little effort and understanding of what the agent needs to know to do an effective job. The problem might be resolved by an action as simple as giving the purchasing agent more complete details and specifications for the item needed.

Experience has shown several pitfalls in the purchasing process can be avoided. Some of these are discussed in the guidelines presented here.

Preparing Specifications

Preparing detailed performance specifications should be the first step in the procurement procedure. For some items, it may be necessary to describe in detail a precise design, measurement, tolerance, material or method of testing or inspection.¹⁸ Suppliers will offer an item which meets only the minimum requirements specified in the invitation for bid (IFB). They will not cut their profits by offering more than is actually specified. For example, a small police department ordered a camera without detailed specifications. The camera body was received without lens, carrying case or other accessories. These items were not included because they are not built-in parts of the camera, and are always ordered separately, through technical descriptions not specified; in this instance, it took several more weeks to order and receive the necessary lens and accessories.

Procurement is usually done competitively, and specifications should not favor one supplier over others. However, the department may contact several potential suppliers for informal discussions and product information. The purchasing agency may be able to furnish reference lists of reputable suppliers, and both professional security journals and telephone directories are also good sources. It is important to use more than one or two sources in looking for a supplier.

Most county purchasing agents will help draft specifications. Many counties have procurement regulations and directives on preparing specifications, and the sheriff should provide the appropriate technical information. Some purchasing agencies use standard specifications for items purchased regularly. If these do not meet departmental needs, the sheriff should provide data to justify changing the specifications and insist they be changed.

Special Provisions in the Invitation for Bid (IFB)

The invitation for suppliers to bid should show complete specifications and any special conditions affecting the procurement, which cannot be added after the IFB is issued. The latter may include:

- Time limit for delivery;
- Phased delivery schedule;
- Requirement for vendors to provide a sample of the item offered for testing and evaluation;
- Requirements for final inspection before acceptance and delivery;
- Citation of minimum standards established by a recognized authority, such as Underwriters' Laboratories; or
- Conditions for warranty certification by vendors, such as ability and willingness to contract for service and maintenance and the availability of service locally or within a specified distance.

¹⁸ Coordinating Committee on a Model Procurement Code for State and Local Governments, *A Model Procurement Code for State and Local Governments, Preliminary Working Papers No. 2* (Washington, DC: American Bar Association, June 1977), p. 73.

Only the purchasing agent can approve requests for exceptions to the IFB, and any exceptions on technical matters should have the sheriff's agreement. If exceptions to the provisions are granted to one or more bidders, all bidders should be notified.

If specialized training by the successful bidder is needed to maintain and operate new equipment, this requirement should be included in the IFB. Training should be scheduled to be completed by time of delivery. Suppliers often provide training during the manufacturing phase so that trainees learn by working on the actual equipment they will be using.

Other Provisions

First, arrangements should be made with the purchasing agent for the sheriff's office to review all bids submitted. This allows a technical overview, and is not meant to preempt the purchasing agent's authority to award the contract.

Second, service and maintenance contracts should be bought from the seller of the equipment. The firm should have the best product experience, trained service staff and spare parts inventory.

In some cases, a purchase from a specific company may be appropriate, rather than receiving competitive bids from several companies. County policy on this "proprietary procurement" should be carefully reviewed before it is requested. This type of procurement might be justified under one of the following circumstances.

- The proposed purchase is part of an approved equipment standardization plan.
- The item is not available from any other source.
- Only the item supplied by a specific firm meets the required specifications.
- Spare parts and special tools are on hand, and buying the item from a different source would require an additional stock of parts and tools.

EQUIPMENT USED FOR COURT SECURITY

The demand for improved security equipment has increased rapidly, as has competition among manufacturers and distributors. Research and development has resulted in many new or improved products. However, the market also is flooded with shoddy, poorly functioning items primarily designed to cash in on the boom by selling to the uninformed or unsuspecting. This section discusses some of the more common types of equipment in use today, focusing only on court security rather than all types of security equipment.

Hardware and Locks

An easy and inexpensive way to improve security is to replace inferior locks and hardware with quality items. During remodeling or new constructions, the additional cost is usually negligible if security planners insist on these items. The following types of equipment should be considered:

- Key-operated locks on windows;
- Door locks with removable cylinders allowing keys, but not entire lock, to be changed periodically;

- Dead-bolt locks with at least a one-inch throw;
- Specially armored locks made virtually break proof for external use;
- High-quality padlocks with changeable combinations;¹⁹ and
- Keyless push-button locks to secure entry into restricted areas (preset combinations can easily be changed by installing replacement slides).

Adequate security does not depend solely on having the right equipment; proper use also is critical. For example, padlocks should always be locked onto the hasp when a door is open to prevent unauthorized substitution of a similar-looking lock. All keys should be under a key-control system managed by the security officer. Simple systems are available from commercial sources for as few as 25 or more than 2,500 keys.

Lighting

Interior fixtures should not be used outdoors because they are not weather resistant and are highly susceptible to vandalism. It is best to seek advice from an electrical contractor to select proper fixtures, cable, wattage output for lamps, and the best means of installation. Fixtures placed at an improper location or at the wrong angle may make coverage inadequate by creating areas of darkness in the overall illumination pattern.

Within the courthouse and courtroom, a wide variety of portable lamps is available for emergency lighting. A commonly used and economical auxiliary or reserve lighting system consists of battery-operated, wall-mounted lamps connected to the existing electrical circuit. The batteries in these lamps are rechargeable and on a constant trickle charge. When the main power system fails, the lamps automatically switch on. Interior courtrooms without windows are often wired with two circuits so that even when the primary lights are switched off, the second circuit will sustain sufficient illumination. The use of key-operated switches for courtroom and holding area light also is recommended. These prevent disruption by unauthorized persons switching off the lights.

Bars, Grilles and Doors

Extra protection should be provided for windows and other openings not normally guarded. Expanded metal grilles or steel bars offer the most economical way to secure these openings. Glass bricks are an alternative method in window openings not needed for ventilation.

Most forced entries are made through windows or doors. If a door is too fragile, it can be broken easily or the lock forced from its strike plate. Solid wooden doors should be at least 1¾ inches thick for all exterior doors; metal or metal-reinforced doors offer even better protection. Any window needed in a door should be of tempered glass or shatter-resistant plastic. Double-cylinder, double-keyed locks should be used on doors having any glass. Local fire codes also must be considered.

Safes and Vaults

Safes have been rated by the Underwriters' Laboratories for resistance to fire and penetration. If possible, safes should be securely fastened to a surface of the building;

¹⁹ These are in use throughout the federal government and meet rigid standards

this is easiest to do in newer facilities with concrete floors. Upon request, safe manufacturers can offer additional advice on immobilizing safes.

Vaults are expensive and should be built by professionals and only if a cost effectiveness study supports the need for them. Manufacturers of vault doors often give advice on design and construction and may even provide architectural drawings to ensure their products will fit properly and function well.

Alarms

The Underwriters' Laboratories²⁰ also have approved alarm standards, developed by a committee that includes representatives from alarm manufacturers, insurance companies, and the Underwriters' Laboratories. The standards are revised periodically and represent the *minimum* acceptable requirements for the design and performance of alarm equipment. Actually, products often exceed these standards, so one system may be far superior to another in actual performance although both are rated the same.

Alarm systems usually fall into one of these four categories:²¹

1. *Local Alarm System.* A system in which the protective circuits in the secured area are directly connected to a bell or siren. The sounding device is prominently displayed on the outside of the building. The bell is fully protected against weather and tampering, connected to the control panel by tamper-proof cable, and audible for at least 400 feet.
2. *Central Station Alarm.* A system in which the secured area is directly connected, via a pair of leased telephone wires, to an alarm panel in a centrally located alarm receiving station. Generally, this system is run by a private security firm. Upon receiving an alarm, the company dispatches its guards to the secured area and notifies the police. Alarm installations of this type can only be approved by Underwriters' Laboratories when the protected premises are within 10 minutes traveling time from the central station.
3. *Proprietary Alarm.* An installation similar to a central station alarm, except the alarm panel is located within a guard room maintained for the owner's internal security operations. The guards operate the system and respond to all alarms.
4. *Police Connection.* An alarm monitor installed in a nearby police station and directly connected to the alarm system via a pair of telephone wires. The alarm also can be connected to local or proprietary systems for additional protection.

Alarm systems used for courtroom security have features from one or more of the above categories. Many courtrooms are equipped with duress alarms, which the judge, court officer or clerk can use to summon help during emergency situations. These alarms

²⁰ The standards are set forth in several pamphlets available from the Underwriters' Laboratories, Inc., Publications Stock Department, 333 Pfingsten Road, Northbrook, IL 60062. See for example, #609 and 610, *Burglar Alarm Systems, Local*; #611, *Burglar Alarm Systems, Central Station*; #636, *Hold-up Alarm Systems*; #681, *Installation, Classification and Certification of Burglar Alarm Systems*.

²¹ Robert Rosberg, *Guide to Security Alarm Systems* (Wayne, NJ: Mosler, Electronic Systems Division, 1978), p. 3.

are inaudible in the courtroom and sound at a manned post that can dispatch a response force. In the alternative, the alarm in a courtroom may be a simple buzzer terminating in the sheriff's office, jail or communications/command center.

For multiple courtroom buildings, many options are available in a wide price range. Many large jurisdictions use a system, which allows two-way voice communication and audio monitoring of the courtroom when the alarm is activated. In another system, courtroom telephones become microphones when the alarm is activated to allow audio monitoring at a terminal point.

Other jurisdictions use a panel of colored lights to alert a monitor and show what kind of incident is taking place – *e.g.*, escape attempt, disorder or hostage situation. However, many systems in use today only alert the security force that an incident has occurred, with no other information given. The alarm monitor should show the origin of the alarm (*e.g.*, the courtroom, chambers or treasurer's office).

As far as technology will allow, a system should include a means to confirm that the signal is not a false alarm. After all, the effectiveness of an alarm system is directly related to how believable it is, and systems with very high false alarm rates eventually may be disregarded by those who must respond to them.

Because of the variety of alarms and alarm systems available, it is important for planners to pinpoint their needs and state their performance requirements clearly before any purchase. Without this caution, it is possible to purchase either too much or too little alarm capability.

Following are a few general guidelines for buying an alarm or alarm system.

- Deal with a reputable company. These will usually be listed by the Underwriters' Laboratories or reputable trade journals.
- There is no such thing as a burglar-proof system, so be suspicious of any sales agent who claims to sell one.
- The system must have a reserve power source in case the main power is shut off.
- Do not buy or lease a system from a company that does not offer a contract for continuing maintenance and service, usually on a two- to five-year basis.

The next sections describe different types of alarm systems for court buildings.²²

Premise Alarms

Premise alarms protect doors, windows and other openings by means of contact devices, switches and metallic foil tape. In some instances, wired wood dowel screens are used instead of metallic foil to protect windows, transoms or similar openings. The screens are arranged to form a continuous closed-circuit loop connected to alarm relays in a control cabinet in the secured area. If anyone tries to enter through one of the protected points, the circuit will be broken, and the alarm set off.

²² *Ibid.*, pp. 4-15.

Capacitance Alarms

The protected object acts as part of the capacitance of a tuned circuit (as a capacitor or condenser). If a change occurs in the region of the protected object (*e.g.*, if someone approaches), there will be a sufficient change in the capacitance magnitude to upset the balance of the system and cause an alarm. Capacitance alarms are used to protect objects that require a high degree of security, such as safes, file cabinets, and other metallic storage containers. The system is fairly flexible, and can be used to connect several items in the same area to one alarm.

Photoelectric Alarms

Photoelectric cells or electric eyes normally are used with other forms of alarm equipment. Its operation depends upon the interruption or breaking of a beam of light between a projector and a light-sensitive receiver some distance away. When the light is cut off from the receiver, an alarm relay is activated in a control cabinet within the secured area. Since white light is easily detected, infrared beams are better for these systems.

Ultrasonic Systems

The protection of an enclosed space can often be achieved effectively by using space alarm equipment. The best known type of system in this category is popularly called ultrasonic; although it actually operates just within the upper limits of the audio frequency spectrum. The apparatus generates a train of high-frequency sound waves (too high for humans to hear) which fill an enclosed area with a pattern of standing waves. A sensitive receiver connected to an electronic amplifier picks up the waves. If they are of the same frequency as the sound emitted by the transmitter, the system will not sound an alarm. Any motion within the protected area will send back a reflected wave differing in frequency from the original transmission. This change in frequency is detected and amplified in the control unit, and the alarm signal is activated.

Audio Systems (Rooms)

Audio systems, unlike ultrasonic, can tolerate air movement and other types of motion as long as the noise created is relatively low. Where fans or other noise-producing items are a fixed part of the room, cancellation microphones located close to the noise-producing items can nullify those sounds. The sensitivity of these systems can be adjusted to detect a very small amount of noise; however, in most installations, this adjustment will result in false alarms.

Audio Systems (Vaults)

The detection of sound or vibration caused by an attack upon the walls, ceiling or floor of a protected structure is the primary function of this system. A microphone and amplifier are installed within the secured enclosure. Sensitivity is adjusted so that normal

sounds will not trip the alarm. However, noises above this level will be amplified enough to activate the alarm relay.

Because the system responds to all noises within the audible range, it is best adapted to vaults or other solid-walled enclosures which require a reasonable amount of force to enter. Most bank vaults are protected by audio alarm systems. These bank installations represent the highest grade of alarm systems recognized by Underwriters' Laboratories.

Radar, Sonic or Microwave Systems

Radar units are generally used to protect interior areas. The principles used in this system closely parallel the operation of the ultrasonic system, with some notable exceptions. Radio waves are highly penetrating and not easily confined within a closed area, such as a room or building. A train of waves is produced and partially reflected back to the antenna. If all objects within the range are stationary, the reflected waves return at the same frequency; if they strike a moving object, the waves return at a different frequency. The difference in the transmitted and received frequency appears as a low frequency signal which is detected and used to trip an alarm relay. The area covered by the radiation field may be controlled by the number or placement of antennas, while sensitivity is controlled by adjusting the amplifier.

Communications

Since so many types of communications equipment are available today, it is important for planners to assess their needs, and the performance they want. Many manufacturers will provide free consultation to help in this task. The following questions should be considered when adding communications equipment to a court security system.

- Is the new equipment compatible with existing systems?
- Are maintenance and repair easily available at local facilities, or must items be returned to the factory for service?
- Is the equipment powerful enough to function effectively in the courtrooms and courthouse?

Ideally, each court security officer should have a portable, hand-held transceiver (radio transmitter-receiver) which is linked to a central command station of the sheriff's base station. If traffic is heavy on the sheriff's assigned frequency, another compatible frequency should be obtained and monitored by the base station. In larger departments, transceivers are usually supplied to supervisory personnel and key officers only. The Law Enforcement Standards Laboratory of the National Bureau of Standards has developed standards for personal portable FM transceivers; these are available upon request.²³

If transceivers are beyond the department's budget, less expensive one-way receivers are available. Even lower in price are the individual "pager" or "beeper" units

²³ NILECJ-STD-0203.00, October 1974, *Personal/Portable FM Transmitters* and NILECJ-STD-0208.00, October 1975, *Personal/Portable FM Receivers*. See Appendix J for information on obtaining copies.

which, when activated, notify the wearer to call a predetermined phone number or take certain actions.

Also available are devices that can be worn unobtrusively or carried in a pocket. When activated, they transmit a radio signal notifying a base station of an emergency situation. These devices have been used by judges and others under the threat of kidnapping or physical violence. They have obvious limitations, including their high cost and short range of signal transmission. Also, since those wearing the devices may be on the move, determining their exact location is not usually possible.

Magnetometers & Density Sensors

Magnetometers come in three basic models: permanently installed, portable walk-through and hand-held. Some of these detectors locate only ferrous or iron-bearing metal. Costs vary widely according to quality and performance.

A combination of walk-through and hand-held models is sometimes used in courthouses. The first type signals the presence of a metallic item, and the second determines its exact location.

The quality of magnetometers varies widely. The U.S. Secret Service and the U.S. Marshals Service have tested various models and identified the ones meeting their requirements. In addition, the National Bureau of Standards has developed standards for magnetometers; these are available upon request.²⁴

Magnetometer like devices are now available that look at the density of items not just metal and walk-thru X-Ray machines are being utilized as well.

X-Ray Screening Devices

These devices are used throughout the world and come in many configurations. Small portable units for screening mail and small packages use drawers that can accommodate items up to 18" x 12" x 16". Larger units are stationary and pass items by the screening device on a conveyor belt. Although these devices are highly effective, cost is the principal factor limiting its use. Thus, they are not practical for departments with limited budgets. Only densely populated urban jurisdictions have a large enough volume of items to screen to justify such equipment.

Explosives Detectors

Explosive detectors are usually portable and the size of small suitcases. They are highly sensitive to vapors emitted by explosives and respond to vapor traces preprogrammed into a unit's memory. Some early models gave false reactions to such items as shoe polish, deodorants and perfume. However, later developments have increased sensitivity and selectivity, largely eliminating this problem.

²⁴ NILECJ-STD-0601.00, June 1974, *Walk-Through Metal Detectors for Use in Weapons Detection* and NILECJ-STD-0602.00, October 1974, *Hand-Held Metal Detectors for Use in Weapons Detection*. See Appendix J for information on obtaining copies.

Tear Gas

Tear gas has been standard equipment for law enforcement agencies for a number of years. The CN gas formula largely has been replaced by a more potent and faster reacting CS gas. Manufacturers supply both types in many configurations and delivery systems, the most common being grenades, projectiles fired from special guns, high-volume bulk dispensers and hand-held dispensers.

Adequate storage space with temperature and humidity control is necessary. Most tear gas items have a known shelf life, and its effectiveness and reliability diminish when these limits are passed.

Many courts have strong feelings about tear gas, and it should only be used in accordance with established policy. Similarly, many sheriffs' offices make the hand-held dispenser either optional or required personal equipment; others forbid its use.

Bullet-Resistant Plastic

Court security planners are increasingly using transparent bullet-resistant plastic shields in courtrooms. For some high-risk trials, a temporary or permanently fixed barrier is placed between the spectator section and the well of the court. A 12- to 18-inch shield is sometimes placed around the top of the bench for the judge's protection.

The two principal plastics used are polycarbonate and acrylic. Acrylic sheets can be shaped to various forms, while polycarbonate is a rigid molded plastic. Acrylic also offers better light transmission: 92%, compared to 66% for polycarbonate. By comparison, bullet-resistant glass transmits only 55% of white light. Underwriters' Laboratories have rated both plastics for bullet resistance, and 1¼ -inch acrylic is rated highest for resisting bullets from medium-power small arms, including .45 ACP, .38 super auto and 9 mm Luger. Note that both these plastics are combustible; building codes should be checked before they are used.

Body Armor

Body armor comes in many forms, including metal or ceramic inserts, chain mail and ballistic cloth. Information is available from suppliers of police equipment and manufacturers of the basic material used. A recent development in the body armor field is the fabrication of synthetic cloth fibers with ballistic characteristics. When woven into cloth and configured for body protection, this material allows a freedom of movement not previously possible.

The Law Enforcement Assistance Administration (LEAA) sponsored a program in July and August 1977 to develop lightweight, continuous-wear, inconspicuous and limited protection garments for public officials and law enforcement personnel. The program led to recommendations on materials and the construction of body armor to meet these objectives.²⁵

²⁵ *Body Armor Program: Executive Summary*, presented by the Aerospace Corporation for LEAA's National Institute of Law Enforcement and Criminal Justice, July-August 1977.

Bomb Disposal Items

The recent increase in bombings of public installations has resulted in many new devices to dispose of explosives. Some are gimmicks, but most are serious attempts to give law enforcement agencies additional tools to handle this dangerous problem. The devices range from simple bomb blankets and baskets for moving suspected explosives to remote-controlled, self-propelled vehicles which, when operated by qualified technicians, can open suspicious packages and remove the contents.

Unless the potential bomb threat is significant, only minimal disposal equipment should be bought. An experienced bomb disposal technician should help develop a list of required items. If the sheriff's office does not have such specialist skills, nearby resources should be tapped, such as another sheriff's office or a U.S. military base.

Closed-Circuit Television

Closed-Circuit Television ("CCTV") systems are available in all price ranges and capabilities, and are usually designed to meet individual needs. Cameras range from simple, fixed installations to remote-controlled units requiring minimal light and equipped with a telephoto or zoom lens. Some systems also have audio capabilities.

For certain purposes, the CCTV system should be operated 24 hours each day. However, for the court security system, the need is usually only for the hours the court is in operation. Still, there is a built-in requirement for people to monitor CCTV systems. Thus, CCTV is not a simple answer to a problem and should be considered only after careful study. As with other equipment, the availability of service, maintenance, and repair facilities should be considered before purchase.

Firefighting and Detection Equipment

Increased incidents of arson in public buildings make installation of firefighting and detection equipment a good investment. Although the purchase and maintenance of this kind of equipment is the primary responsibility of a building engineer, manager or custodian, the security officer should ensure that minimum local fire codes are met. The National Fire Protection Association has available, for a nominal cost, standards for various types of fire alarm systems.²⁶

Dogs

Dogs also can be used effectively in a court security operations plan. The animals can help deputies in weapons, drugs and bomb searches, as well as building patrol and crowd control. However, the expenses and other problems incurred by the need for retraining, feeding, housing and general maintenance limit the suitability of dogs for most offices.

²⁶ Contact the National Fire Protection Association, 470 Atlantic Avenue, Boston, MA 02210

CONCLUSION

Equipment purchases can be made more cost-effective by observing the suggested guidelines in this chapter. To summarize, procurement can be placed on sound footing by following a few general guidelines:

- Identify needs;
- Prepare clear and complete specifications;
- Seek professional guidance when needed;
- Balance manpower and specialized training needs against equipment purchases
- Develop sound maintenance and service contracts; and
- Maintain a good working relationship with the county procurement officer.

CHAPTER 6

PERSONNEL AND TRAINING

This chapter assists security administrators in developing standards for personnel selection, assignment and use, as well as how to update or start a training program. The guidelines here are addressed to managers, while details for the training officer are in supplemental training material (see NSA's 1978 publication, *Court Security Training Guidelines*).

Good personnel and effective training practices, policies and procedures are essential to any organization. Yet standards for both personnel and training vary greatly among criminal justice organizations. Many states have recognized this, and have established minimum training standards for law enforcement personnel. However, state training programs often have little, if any, discussion of court security.

One reason for the differences in selecting and training court security personnel is the number of different agencies responsible for court security. Even within a single jurisdiction, specific court security responsibilities may be unclear or shared by judges, court administrators, court clerks, local law enforcement agencies and the sheriff. For example, some managers may want to fill a job with law enforcement officers, while others want civilians. This makes it hard to establish uniform standards for personnel and training.

PERSONNEL

Selection and Assignment

Standards for personnel selection and assignment should be considered within the overall requirements of the judicial system. The need for integrity, discipline and dignity in the courtroom means security staff should be aware of certain laws, customs and standards of conduct. For example, an inappropriate remark by a court officer to a juror can cause a mistrial, and unnecessarily rough handling of a defendant in court can produce a violent response. Proper personnel selection and training programs can prevent such situations.

Specific responsibility for court security should be identified and assigned to a single department, if possible. Then, as a first step in developing standards for court security personnel selection and assignment, managers can identify tasks and responsibilities for each position.

Next, managers should develop detailed court security position descriptions, including the following information:

1. Specific description of work to be performed, by tasks;
2. Operating responsibilities and authority;
3. Requirements for communication and coordination among security personnel;
4. Supervisory responsibilities and lines of authority; and

5. Experience, skill and education requirements and standards for both new personnel and individuals being considered for reassignment or promotion.

County officials, such as civil service officers, should be consulted to make sure these position descriptions are consistent with county personnel practices.

In a sheriff's office, officers assigned to court security usually will be selected from within the office. Other agencies responsible for court security probably will have to recruit new people. Whether court security officers are new or reassigned employees, selection standards should be carefully detailed and should reflect appropriate federal, state and local laws, including requirements for equal job opportunities.

Unusually high standards may discourage potential candidates from applying for vacant positions or may be so unrealistic many applicants are unfairly eliminated from consideration. Then too, the people hired may find the work does not match their expectations. As a result, both finding and keeping competent persons can be a challenging task for a manager.

Selection standards should reflect the minimum qualifications needed to perform a job. The recruitment base should be as broad as possible, since personal interviews and written examinations will identify the best qualified applicants.

To get people with the right skills, recruitment should be aimed at university graduates, other law enforcement agencies and military personnel. Selection and placement standards should focus on psychological makeup, attitudes and the ability to cope with stress, as well as physical ability and intelligence. Once an individual is hired, a good training program can help develop or improve the skills needed to perform certain tasks, but few training programs can successfully overcome individual psychological problems.

In many courtrooms, the security officers are not able to respond well to physically and mentally strenuous situations because of age, physical condition or lack of proper training. These situations are potentially hazardous not only to the officer but to everyone else in the courtroom. Court security is only as good as its weakest link, and using unqualified personnel is risky.

Criteria now used to assign court security officers include (1) physical inability for other assignment, (2) assignment as a disciplinary measure, (3) personal preferences of judges or the officers themselves, and (4) efforts to make the assignment part of overall career development. These may or may not be valid points to consider in assigning an individual to a position, but personnel should meet established standards or their work may be inadequate.

Effective Use

After selection and assignment standards have been set, personnel must be used properly if an operation is to be effective. Sometimes court security officers are used for nonsecurity tasks, including court clerk duties and personal tasks for judges, court clerks or court administrators. This practice not only contributes to job dissatisfaction and possible high turnover rates but also decreases the number of officers available for security.

Managers should view court security assignments as an important position in the career development of all officers. Ideally, an office's career development program should include individual counseling and assignment to various tasks within the office. The objective will be to develop a broad base of experience and increase promotions. Assignment as a court security officer should be considered a part of career development, with the length of assignment determined by departmental policy or experience. The absence of such a program may eventually cause a lack of personal interest in professional development.

Evaluation

Many court security officers are not evaluated regularly, and even departments having an evaluation program often fail to recognize its value as a management instrument. A personnel evaluation system administered fairly to all employees can identify (1) people with leadership and/or problem-solving abilities, including those ready to assume greater responsibility, and (2) employees who are having problems with interpersonal relationships or high-pressure situations. Evaluation gives both employees and supervisors a chance to discuss their problems. For example, an officer may feel he is being denied a promotion because of duties with little or no relationship to court security. Thus, all duties should be described in the evaluation, even such tasks as running personal errands for a judge. Such description provides a guide for evaluating performance.

If the office does not have an evaluation system, the manager should find out if one exists for other county employees. If so, the manager may be able to adapt that system to court security personnel.

TRAINING

Most administrators of security-oriented agencies know training is critical. However, this key activity depends upon such factors as the availability of funds; training resources and space; the number of people who can be taken away from their assignments; and state training requirements.

Even when states require a specific number of training hours for law enforcement officers, court security usually is not included. Some state laws require specific hours of training in court security, including firearms and less lethal training.

Almost all sheriffs contacted during this project acknowledged the importance of court security training, and even the most sophisticated departments recognize the need for a more structured training program. In most jurisdictions, instruction now given on court security is limited to on-the-job training.

Management Considerations

The manager must examine any training program in terms of office needs, costs and how effective the proposed training will be. This section sets forth key training considerations and guidelines.

The more effective the training program, the greater likelihood personnel will be to carry out their responsibilities at the least cost to the office. With good training,

managers have maximum flexibility in using personnel, since they can assign staff on the basis of both ability and need.

At the same time, an important aspect in personnel assignment is the manager's awareness of strengths and weaknesses among employees. Some are more adept at certain tasks than others, regardless of the amount of training. A sound training program will measure those strengths and weaknesses and will allow managers to assign personnel where they can be most effective. Managers also can take steps to correct weaknesses and develop or improve employee capabilities, either through further training or career development assignments.

An important and often overlooked management consideration is the liability office administrators assume for the actions of those working under them. If an employee causes injury or property damage, either by action or inaction, both employee and supervisors may be legally liable. However, liability can be limited if a manager can show that the employee was properly training and adequately supervised. Therefore, office files must include information on the kind of training provided, when it occurred, training scores (*e.g.*, firearms qualification scores), and other examination results.

A manager should see that an office operates at the least cost for optimum results. Training costs should be included in the annual budget for space, staff salary and operating expenses, and the administrator should review those costs before the budget is finalized.

Initial costs for a training program include equipment, reference books and related supplies and materials. Note it may be more efficient to get training aid from someone outside the department. In such case, the cost should be examined after a complete evaluation of an office's resources, as well as the need for training to make sure the expenditure is essential.

Developing a Training Program

Managers should take the following initial steps in developing a new training program:

Describe the importance and priority of the program in an office policy statement. Because training involves all personnel, they should be prepared to participate in the program, and should recognize the priority given to training by the administration.

List the goals of the training program and groups within the department whom will benefit. A typical overall statement would be: "The goal of our training program is to provide essential instruction each year to all members of the department on the broad duties and responsibilities of the department." The statement should also identify specific objectives to meet the overall goal.

Training often is considered useful only to new staff. However, all employees need to update skills and abilities. Even supervisors can benefit from training, which helps them keep informed of the latest technique and procedures for management, administration and supervision. Thus, a training program should be based on both the goals statement and the identification of target groups benefiting from the effort.

Select a training officer. In larger departments, it may be necessary to assign this key role to a person who has no other duties. In smaller departments, this may not be

possible, but, in either case, it should be clearly understood that the training officer will do the following:

1. Directly respond to the department administrator;
2. Communicate with all department units, keeping them informed of what the training program involves and seeking their views on training needs;
3. Develop the training plan, and get it approved by the administrator;
4. Determine program costs and prepare specifications for all supplies and equipment to be purchased;
5. Design the program;
6. Assign personnel to the training classes, with guidance from appropriate department officials (*e.g.*, the personnel officer);
7. Manage the delivery of training, conduct class examinations and keep performance records;
8. Evaluate the training program at the end of the course and write a post-training report (if required) for the administrator.

Some states require certification of law enforcement instructors within the state education system. Training officers should be state certified when appointed, or they should become certified as soon as possible thereafter, since certification is usually necessary to obtain academic credit for the training.

Some people seem to have natural talent as trainers. Standards to identify those persons often are intangible, but generally include their attitudes toward training, and the degree of satisfaction they get from being trainers.

Training officers should have field experience in the subjects they might teach. While the training officer in a large department may not do much direct teaching, this will not be the case in most jurisdictions. Thus, the trainer should be an experienced officer who has the professional respect of the class.

Ideally, training officers will have senior rank in the department. They will be links to senior department staff and to appropriate court officials, including judges, court administrators and prosecutors. They will sometimes be principal assistants to chief administrators. A senior, experienced officer will be most able to command the respect needed in these relationships.

Sometimes employees will feel that full-time assignment to training can provide professional opportunities and a greater opportunity for advancement. However, the opposite also may be the case, and training officers may feel they are outside the mainstream of promotion opportunities. An administrator should take any necessary steps to lessen such fears and ensure that no one's career development suffers by being heavily involved in running a training program.

Locate available training resources. Managers should look at several sources of information and possible assistance, including nearby sheriffs' and police departments, federal agencies or universities with criminal justice programs. These sources may be able to suggest ways to plan and carry out court security training programs. Nearby jurisdictions also may have equipment or visual aids, such as films or slide presentations, and these could be borrowed to reduce the training program's cost.

The Training Plan

The first major responsibility of the training officer is to develop a training plan, which involves the following steps:

1. Complete a work or job analysis of prospective trainees and learn required performance objectives;
2. Define the goals of the training program, as learned from the work analysis and other management requirements;
3. List training targets – *i.e.*, names or categories of people to be trained, including subjects to be taught.
4. Describe the training topics, including the scope and nature of each;
5. Define the training resources needed, such as instructors' names (biographical data in some cases) and supplies.
6. Describe the training strategy, including ideas for achieving the office's training goals, and a discussion of the planning considerations that led to the proposed training program. For example, the training strategy may be to train everyone in the department. To do this in the shortest possible time, one approach may be to offer both recruit training for new personnel and refresher training for existing employees, including supervisors;
7. Prepare a training schedule, showing the time each subject is to be taught. Training might be needed in shorter time periods or during off-hours if trainees cannot be spared during work hours. This practice will usually involve overtime pay, so the administrator may want to discuss other options with the training officer before approving this step;
8. Prepare an estimate of costs for the entire program, including those for overtime (if needed), travel, subsistence, lecture fees, supplies, printing and visual aids. If a yearly plan is submitted, these costs can be included in the budget after approval by the administrator.
9. Evaluate the program by drawing up a plan for "before-and-after" testing to look at the training program's effectiveness in meeting departmental goals.

Management Control

If administrators give training high priority and make this view known to their staffs, the department generally will reflect that attitude. Obviously, the reverse is also true. Thus, administrators play a major role in convincing department staff of the importance of training and in assuring that training contributes to effectiveness and efficiency in their departments.

An administrator also controls the ongoing development of the training program through frequent meetings with the training officer and by approving each training plan. In this way, the administrator makes sure the program will meet department needs at the least cost.

The administrator's approval of the training plan, including the cost estimates, represents a step in the budget preparation process. The budget's line item for training reflects the approved estimates. By listing those costs as a line item, the administrator can better decide priorities and necessary funding levels.

Finally, the evaluation process is very important. Here again, administrators have a major task because they must review the results of the evaluation and be sure that changes are in line with office priorities and effectively meet training needs.

CONCLUSION

People are the main factor in any security program. Equipment, procedures and architectural security measures are meaningless without capable and trained staff to use them. Thus, effective selection, assignment and training are vital parts of a successful security program, as are sound management and control of all training efforts.

Appendices

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Is the entire perimeter lighted?				
Are lights on all night?				
Are lights controlled manually?				
Are lights automatically controlled?				
Are light control switches secured?				
Do exterior lights have an auxiliary power source?				
Do perimeter lights have an auxiliary power source?				
Date exterior lights last tested?				
Date perimeter lights last tested?				
Excluding parking areas, describe the lighting conditions of building grounds (fully, partially, poorly or not illuminated)				
Is the building exterior sufficiently lighted to discourage and observe unlawful entry and placement of explosive devices?				
Are public areas sufficiently lighted to discourage and detect assaults on persons?				
Do landscape features provide places for potential intruders to conceal themselves?				
Are there items that could be used by intruders to gain courthouse access and/or commit assaults?				
Are all area shrubs trimmed down to maximum height of than three feet?				
Are all area trees trimmed up to a minimum height of six feet?				
Is there adequate natural surveillance from adjacent properties or roadways onto the courthouse property?				
Is signage effectively used to direct visitors to the public entrance?				
Are signs or notices clearly posted informing the public of contraband violations and the screening methods for such items?				
Are tree limbs trimmed back at least 10 feet from the fence?				
Is the fence line regularly inspected for signs or tampering or needed repairs?				
Is "No Trespassing" or other signage posted along fencing?				
Are all exterior doors and windows equipped with cylinder locks, dead bolts, dead latches or GSA high security padlocks?				
Are all hinge pins internally located, welded, or otherwise secured from easy removal or are high security hinges used?				
Are all unused doors permanently locked?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are window bars/mesh securely fastened to prevent removal?				
Are windows on the ground floor protected by security film?				
Are openings to the roof (doors, skylights, etc.) securely fastened or locked from the inside?				
Is internal access to the roof controlled?				
Is the roof accessible from the exterior of the building?				
Are roof openings integrated into the alarm system?				
Are openings to the building (e.g., tunnels, utility and sewer manholes, culverts, service ports) properly secured?				
Is a key/card control system in effect?				
Is there a primary individual responsible for the key/card control system?				
Are building entrance keys/cards issued on a limited basis?				
Are master keys/cards secured and issued on a strictly controlled basis?				
Can the key control officer replace locks and keys/cards at their discretion?				
Must duplication of keys be approved by the key/card control officer?				
Can access cards be deactivated remotely?				
Is the number of access points reduced to the minimum necessary?				
Do judges and court officers have a private entrance to the building?				
Do all walls extend fully to the ceiling?				
Do exterior walls extend to the decking?				
Are solid ceilings used?				
Are private elevators provided for judges?				
Are certain elevators used exclusively to move inmates?				
Are inmate elevators marked "Not for Public Use"?				
Are inmate elevators controlled by key/card?				
Are prison elevators programmed to bypass certain floors?				
Are inmates placed in the elevator in a separate holding area secured by metal bars or grilles?				
Are inmate elevators equipped with audio or video surveillance?				
Are inmate elevators equipped with a duress alarm or direct line telephone?				
Are weapons, ammunition or riot control chemicals maintained within the building?				
Are hazardous substances such as cleaning agents stored in a restricted area?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are hazardous items stored in a secure room?				
Is the storage area integrated into the intrusion alarm system?				
Is the door in the storage area solidly constructed?				
Are hinge pins concealed or welded to prevent removal?				
Does the door have an adequate cylinder lock?				
Do all windows in the storage area have steel bars, or mesh, or are they permanently sealed?				
Is the storage area well ventilated?				
Is the storage area integrated with the fire detection system?				
Does the storage area have a sprinkler system?				
Are inventories and/or controls used to monitor the loss of sensitive or hazardous materials?				
Is the main power source dependable?				
Is there a dependable auxiliary power source for emergencies?				
Does the courthouse have an intrusion alarm system?				
Does the system meet Underwriters' Laboratories standards?				
Is the system regularly tested?				
Is there a minimum 48-hour back-up battery emergency power source for all alarms?				
Does the emergency power source activate automatically?				
Does the alarm system alert in case of extreme temperature changes within the building?				
Are records maintained of all alarm signals (e.g., time, date, location, cause and action taken)?				
Are all false alarm activations examined for causative factors?				
Does the courthouse comply with local fire codes?				
Does the fire marshal routinely conduct inspections on the courthouse?				
Does the building have an individual fire detection system or is it integrated into the intrusion alarm system?				
If not, does the building have smoke detectors?				
Does the building contain a sprinkler system?				
Does the building have fire extinguishers?				
Does the building have emergency fire hoses?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Have courthouse personnel received proper training in the use of fire extinguishers or fire hoses?				
Are communications between security personnel adequate?				
Is there more than one communications system used exclusively by security personnel?				
Is there more than one communications sytem used exclusively for security purposes?				
Is the public address system utilized as part fo the emergency notification system?				
Can portable radios communicate to other outside law enforcement agencies?				
Do courthouse base radio stations have an auxiliary power source?				
Is there a duress code or signal?				
Are public waiting areas routinely searched and patrolled?				
Are any waiting areas adjacent to courtrooms?				
Are drop ceilings used in waiting areas?				
Are public restrooms routinely searched?				
Are any restrooms next to courtrooms?				
Are drop ceilings used in restrooms?				
Do trash receptacles allow easy concealment of contraband?				
Are directions (directories and floor plans, if apprpriate) clearly posted in all public areas?				
Is entry to and exit from parking areas controlled?				
If automated gates are used, are there measures to control "tailgate entry?"				
Is visitor parking restricted to no closer than 150 feet from the courthouse?				
Is underground parking (under facility) restricted to employees only?				
Are parking areas monitored by video surveillance?				
Are frequent inspections made of parking area(s) and vehicle(s) not guarded or monitored by video surveillance?				
Is there a reserved parking lot on courthouse grounds?				
Is the reserved area closed or locked during non-business hours?				
Is the reserved area protected by a fence or barrier?				
Are signs posted advising of restriction?				
Is there reserved parking for judges?				
Is there reserved parking for court staff?				
Is there reserved parking for jurors and witnesses?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are parking spaces reserved by name or title?				
Are parking spaces reserved by number?				
Is access to the garage strictly controlled?				
Is there direct access for judges from the garage/parking area to non-public elevators or restricted entrance points?				
Is there good natural surveillance from the courthouse interior to the parking area(s)?				
Are all exterior doors at least 1 3/4 inch solid core wood, metal clad or metal?				
If doors are solid glass, is alarm system equipped with glass breakage sensor(s)?				
Are all exterior doors properly equipped with dead bolts or quality locking devices?				
Are doors with windows or glass within 40" equipped with alternative locking devices?				
Are all exterior doors integrated into the alarm system?				
Are all hinge pins internally located, welded or otherwise treated to prevent easy removal?				
Do doors with panic bars have auxiliary locking devices for use when the building is not occupied?				
Are exterior door frames constructed or reinforced to prevent spreading of the frame?				
Are exterior door bolts protected or constructed so that they cannot be cut?				
Are all unused doors permanently secured?				
Are assessable windows properly secured and/or integrated into the alarm system?				
Are window bars/mesh securely fastened to prevent removal?				
Are there separate courtroom entrance/exit points for judges?				
Are there separate courtroom entrance/exit points for in-custody defendants?				
Are there separate courtroom entrance/exit points for the general public?				
Can you conduct a visual observation of the courtroom without entering (windows/door viewers)?				
Are there security guard(s)/personnel on duty after normal working hours?				
Is there a procedure for routine daily inspection of the courthouse?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are there public security screening stations at the entrance of the courthouse(<i>i.e.</i> , magnetometers, wands, etc.)?				
Are courthouse employees allowed to bypass the public security screening stations at the entrance of the courthouse?				
Is there a separate entrance into the courthouse for employees?				
Is the separate entrance for employees monitored?				
Does the courthouse have a public address system?				
Are Fluoroscopes (x-ray) machines available for use?				
Are safes and vaults integrated into the alarm system?				
Are the locations of utility control points known to security or supervisory personnel?				
Are utility and plumbing access plates and doors locked or sealed when not in use to avoid tampering?				
Are basements or crawl space access doors integrated into the intrusion alarm system?				
Are doors or access points to basements, utility rooms, boiler rooms, crawl spaces and attics secured when not in use?				
Are heating and air conditioning fresh air or return vents secure from tampering?				
Are fire detection devices located in the records storage area?				
Is a sprinkler system located in the records storage area?				
Are work records/files stored in secured rooms or locked filing cabinets during non-business hours?				
Are records storage areas accessible to unauthorized persons?				
Are there checkout/accountability procedures for all records?				
Is there a secure area available in or near the clerk's office for the public to review documents?				
Does the cashier's window/desk have security features?				
Is a large amount of cash maintained in the office overnight or on weekends?				
Is there an adequate safe, vault or strongbox?				
Is the safe approved by Underwriters' Laboratories?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are safes weighing less than 750 pounds securely fastened to the floor, wall or set in concrete?				
Are combinations changed when personnel terminate employment?				
Is there a duress alarm in this office(s)?				
Is/are an armed escort(s) used to make bank deposits?				
Is there a standard operating procedure (SOP) manual for the courthouse?				
Is all data current and correct?				
Does the SOP describe the security and control of inmates being transported to court?				
Does the SOP describe procedures for transporting and handling sick, injured, handicapped and mentally ill or inmates suspected of carrying a communicable disease to court?				
Does the SOP describe procedures for the transportation of juveniles or inmates of the opposite sex to court?				
Does the SOP describe procedures following the escape of an inmate while being transported to court?				
Does the SOP describe procedures for the transport of a High Risk/Profile defendant to and from court?				
Does the SOP provide a written directive on the types of restraints authorized by the agency and the circumstances or conditions for their use?				
Does the SOP provide a written directive that all involved personnel receive training in the operation of a lockup/holding cell?				
Does the SOP describe a written directive describing the "security and control" features of the lockup/holding cell(s)?				
Does the SOP describe procedures following the escape of an inmate?				
Does the SOP provide a written directive, consistent with legal requirements, that all inmates be searched upon entry into the lockup/holding cell(s)?				
Does the SOP provide a written directive establishing procedures for instances when a person is placed and left alone in an interview room?				
Does the SOP provide a written directive establishing procedures for who has access to the lockups and who must authorize those individuals that are not normally authorized?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Does the SOP provide a written directive establishing the agencies courthouse/courtroom security function?				
Does the SOP provide a written directive governing the courthouse/courtroom security function must be made available to all personnel assigned therein?				
Does the SOP provide a written directive specifically identifying a position withing the agency responsible for the courthouse/courtroom security function?				
Does the SOP provide a writtend directive governing required searches of courtrooms for contraband?				
Does the SOP provide a written directive specifying that equipment used for courthouse/courtroom security be identified and available for use at all times?				
Does the SOP establish who is responsible for declaring an emergency?				
Is the authority and chain or command clearly defined and in the crisis plan?				
Are all crisis plans subject to periodic review and updating?				
Does the SOP establish a procedure for handling medical emergencies involving the general public?				
Is first aid equipment, including oxygen, provided throughout the courthouse?				
Is that equipment periodically checked and tested?				
Are courthouse personnel trained in the use of first aid equipment?				
Are court personnel given periodic instruction about the various crisis plan procedures?				
Are mutual aid agreements dealing with crisis siutations with other agencies written or informal?				
Are periodic fire and evacuation drills held?				
Are periodic security conferences held with the judge(s)?				
Are period courthouse security reviews conducted with the building's court security committee (i.e. , building users and/or tenants)?				
Does the SOP follow the Department of Homeland Security's National Incident Management Systems (NIMS) guidelines for managing and processing an emergency?				
Are security plans coordinated with appropriate local, state and federal agencies?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are public, private and inmate circulation patters separated and well defined?				
Is there a routine inspection of packages and shipments entering the courthouse?				
Are mail and other delivers received at one central location?				
Are personnel receiving mail/shipments trained in suspicious package identification?				
Are video surveillance camera displays monitored 24 hours?				
Are personnel monitorint displays provided timely breaks?				
Is video monitoring taped or recorded?				
Are tapes or recordings rotated daily and maintained for a minimum of 30 days?				
Do spaces above, below and next to the courtroom present a security hazard?				
Are all unused doors secured?				
Is the inmate entry door far enough from the public seating area to prevent passing contraband?>				
Are all windows draped to obscure vision (particularly of the bench) from outside?				
Is there emergency lighting in the courtrooms?				
Are light keys controlled for lights in the courtrooms?				
Are courtroom lights inaccessible to the public?				
Is the main area or well separated from the spectators by a barrier?				
Is the judge's bench closed at both ends to restrict access from the well?				
Are the defendant's chair and the witness chair built to allow use of restraints?				
Are spectator seats solidly built and fastened to the floor?				
Are potential weapons, such as drinking glasses, water carafes, and ash trays, kept out of the defendant's reach?				
Are metal detectors avialable for use in or near the courtrooms?				
Is the bench reinforced to make it bullet resistant?				
Is there a duress alarm in the courtroom?				
Are duress alarm buttons installed at the bench?				
Does any duress alarm installed at the bench have an audio monitory capability?				
Is there an acceptable response capability for courtroom duress alarms?				
Does the courtroom have a telephone?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Does the courtroom have a public address system?				
Is the bailiff equipped with a portable radio?				
Are additional restraining devices available for use in the courtroom?				
Is there a policy for whom may carry firearms into the courtroom/courthouse?				
Are bailiffs armed in the courtroom?				
Are bailiffs in uniform or identifiable?				
Are inmates kept in restraints except when in the courtroom?				
Are there procedures for the emergency evacuation in the courtroom/courthouse?				
Do bailiffs understand procedures for emergency evacuation of inmates from the courtroom?				
Are judge's chambers routinely searched for contraband by bailiffs and secretaries?				
Is visitor access controlled by clerks, bailiffs and/or secretaries?				
Are suspicious packages or letters examined before delivery to judges?				
Does the judge's chamber have more than one means of entry or exit?				
Do doors have automatic closing and locking hardware?				
Are the chambers routinely locked when the judge is not present?				
When occupied by the judge, are the chamber doors normally unlocked?				
Are outside views, particularly of the judges' desk, obscured?				
Are judges routinely escorted between parking areas, chambers and the courtroom?				
Are judges escorted between parking areas, chambers and the courtroom during high-risk or sensitive trials?				
Are judges escorted between their residence and courthouse during periods of personal threats?				
Does the judge's chamber have a duress alarm?				
Is there an acceptable response capability for these alarms?				
Do any judges carry firearms?				
Do any judges keep firearms in their chambers?				
Do any judges keep firearms at the bench?				
Are witness waiting rooms provided?				
Is it possible to separate prosecution and defense witnesses?				
Is public access to waiting rooms restricted?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are light switches located outside the waiting rooms?				
Are room(s) provided in the courthouse for attorney/client conferences?				
Are these room(s) secure?				
Do/does the room(s) have drop or removable ceilings?				
Can the room(s) be locked?				
Is the room(s) routinely searched for contraband before and after use?				
Are conferences visually observed at all times?				
Is the jury deliberation room next to the courtroom or accessible through a controlled passage?				
Are the windows draped?				
Are restrooms provided as an integral part of the deliberation area?				
Is the deliberation room soundproofed well enough to prevent unauthorized persons from eavesdropping?				
Is the deliberation room routinely searched for contraband before occupancy?				
Is the deliberation room locked when unoccupied?				
Are inmates brought in from outside the courthouse through a private entrance or sally port?				
Is the area equipped with gates that can close the area to the public?				
Is there more than one way for vehicles to exit from the area?				
Are gates electronically controlled from a remote station?				
Is an interlocking system used so that the outer gate can be closed and locked before the door to the building is opened?				
Is this area monitored by video surveillance?				
Is this area used exclusively for inmate movement?				
Is the entrance for inmates out of public view?				
Do inmates walk through public areas when going from temporary holding areas to court?				
Are restricted passages also used by judges and court staff?				
Are restricted or secure passageways monitored by video surveillance?				
Are law enforcement officers required to leave guns in locked cabinets before entering restricted or secure passages?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Are keys to secure passageways issued to people other than court security personnel?				
Are security staff forbidden to remove secure passageway keys from the building?				
Are the stairways used for inmate movement adequately lit?				
Are stairways and stairwells enclosed with protective metal grilles?				
Are stairways monitored by video surveillance?				
Are temporary holding cells located in the court building?				
Do temporary holding cells open directly into the courtroom?				
Are adequate toilet facilities available for inmates?				
Are lights for the holding area controlled from outside the cells?				
Do cells have emergency lights?				
Do cell doors have observation ports?				
Is at least one holding cell equipped for audio and/or visual coverage of courtroom proceedings?				
Are cell doors locked and unlocked from a remote center?				
Are keys to temporary holding cells issued to people other than court security personnel?				
Are temporary holding cells locked with keys that cannot normally be duplicated commercially?				
Are cells and areas used by inmates routinely searched for contraband before and after use?				
Are cells built securely in a way that reduces opportunities for self-inflicted injuries by inmates?				
Are law enforcement officers required to leave guns in locked cabinets before entering temporary holding areas?				
Are inmates kept in restraints except when in the cell?				
Are additional restraining devices available?				
Are telephones/intercoms available in holding cells?				
Are juveniles routinely separated from other inmates?				
Are females routinely separated from other inmates?				
Do inmate feeding procedures present escape opportunities?				

Courthouse Security Plan and Outline

Issue	Yes	No	N/A	Notes
Do security and transportation officers understand procedures for emergency evacuation of inmates from temporary holding areas?				
Are the number of gun cabinets adequate for visiting officers?				

THE ON-SITE COURT FACILITY SURVEY

Once the court security committee has been incorporated and established, a team should be assigned to conduct an on-site survey of the facility to identify what assets are in place, weak areas needing attention, and what can be done to rectify any shortcomings. The survey should be comprehensive and conducted by more than one person to insure that no areas are missed, and to insure a complete and impartial appraisal. An on-site physical security survey can also be arranged through CODA or the U.S. Marshals Service.

The example survey at the end of this manual may be used by in-house personnel to conduct their own internal physical security survey, noting that not everything on this example will pertain to every existing facility, and allowances and adjustments should be made.

The best survey is useless if it remains in a file somewhere without action. The court security committee of a facility should meet immediately following the completion of the survey, and begin steps to review and analyze the current overall security situation of the facility. The representative from the funding source is a critical player in this meeting, as nearly every existing facility will need changes or modifications that are expensive. This fact in and of its self should not, however, slow the committee from taking those steps that can be implemented at little or no expense, and yet make significant improvements in the overall security, such as adding or changing locks, adding window film, signage, simple barriers etc.

The physical security survey will also highlight staffing needs. Convincing the funding source of staffing demands and needs is at best a difficult task without some outside authoritative guideline or source to validate it.

The following “NATIONAL STAFFING GUIDELINES FOR COURT FACILITIES” can be used by the committee to help justify the request for addition staffing.

NATIONAL COURTHOUSE/COURT FACILITY STAFFING GUIDELINES

*Sheriff John E. Zaruba
DuPage County, Illinois*

How much courthouse/courtroom security is too much and is there a formula for an adequate/minimum security force?

The answer comes only after the accomplishing the following steps.

Step One:

Conduct a threat analysis. Assess your historical threats, your current threats and your anticipated future threats. Jurisdictions are similar based on demographics. Research and then assess. Include worker/workplace events. Workplace violence in a judicial setting is 15 times the national average.

Step Two:

Complete an accurate and thorough court facility **site** survey. Assess your facility's external and internal weaknesses. Assess your policy and procedures by testing them. Assess your staff, their physical and psychological abilities, training, commitment and security levels. Assess your practices against CALEA Chapters 71, 72 and 73 standards.

Step Three:

Establish a **security committee** made up of all users of your court facility(s). Now, add to this a member of your funding source (County Board/Commissioners, etc). Review the results of steps 1 and 2 together and jointly decide your course of action. This step will be the most difficult but it will help create a mutual understanding and a mutual direction that will increase your level of security.

During your discussions, these mandatory questions must be answered:

Who is legally responsible for court security?

What is the level of security desired for each location?

Are you going to be gun free? Who is authorized to carry firearms in the facility?

Is security for all or for some? (Passes)

Is funding available now, can security be phased or is this as good as it gets?

Can the eight security zones be segregated physically, temporally, or procedurally? Are they cross-contaminated?

Is staffing adequate to protect and preserve the judicial integrity of the criminal justice system? Staffing is not just people placed in positions. An adequate staffing analysis requires looking at all phases of human resource management.

STAFFING ANALYSIS PHASES

Recruitment

Hiring

Training (*Basic/Specific*) Placement

Retention

Command

The following post assignment staffing guidelines should be used as a general guide for the provision of proper security staffing of your courtroom/facility. The factors which determine adequate staffing for your specific courtroom/facility will be determined by you utilizing steps one, two and three above.

STAFFING GUIDELINES

Large Counties and Cities:

Courtrooms

Civil Court	1
Criminal Court	2 (additional security assigned as justified)
Juvenile	2
Domestic	2
City Court (Traffic)	2

Building Security Posts as delineated by security survey and special justification

Court Facility

Criminal	2
Civil	1
Juvenile	2
Domestic	2

Floor Security 1 (minimum each floor)

Supervisory ratio 1 for every 6 court operations

Unique posts where identified by security survey and special justification

10% relief factor

Small Counties:

Courtrooms/Facilities

Criminal Court	minimum 1
Civil Court	minimum 1
Other	minimum 1

Security position 1 over each court operation per judge

Additional building security positions as identified by court security survey and special justification

10% relief factor

City Courts: (Small)

Courtroom/Facility

Criminal Court	minimum 1
Civil Court	minimum 1
Other	minimum 1

Security position 1 over each court operation per judge

Additional security positions as identified by court security survey and special justification

Superior - Appellate - Supreme Courts

Courtroom/Facility

Criminal Court	3 and 1 supervisor
Civil Court	1

1 senior officer for every four-full time judicial hearing officers

Additional security positions as identified by court security survey and special justification.

10% relief factor

Other Courts:

Courtroom/Facility:

1 full-time security position for each court facility operation

Criminal Court	1.5
Family Court	1.5
Family Court Hearings	1
Civil Court	1

Additional security positions as identified by court security survey and special justification

COURT SUPERVISION (Generally)

1 Supervisor in-Charge for each court facility operation

1 Assistant Supervisor In-Charge for each court that has more than one location with 5 or more regularly scheduled courts or has 50 or more court security officers assigned to a single location

1 Staff assistant for each Responsible Supervisor In-Charge **OR** Assistant Supervisor In-Charge with a maximum of one per facility

1 Supervisor to cover public security entrance

10% relief

ADDITIONAL STAFFING GUIDELINES

Magnetometer/ X-ray Staffing

Magnetometer	2
X-ray	1

Entrance Staffing

Pass line	1
Canine (Bomb)	1

Prisoner Transportation

As necessary based on Risk Assessment

SPECIALIZED STAFFING CONCERNS: (Additional staffing and policy required)

24/7/365 SECURITY (*Preferred*)

MASTER CONTROL

TRAINING

FACILITY RESPONSE

ALARMS

MEDICAL EMERGENCIES

OTHER EMERGENCIES

FIRE OR WEATHER EVACUATION

ESCAPE

ILLEGAL ENTRY

JUDICIAL SECURITY

THREAT ASSESSMENT/ ADJUSTMENT/INVESTIGATION

PROPERTY CONTROL

ARREST/INVESTIGATION/DETENTION

SPECIAL OPERATIONS/DEMONSTRATIONS

FACILITY SHUTDOWN

HIGH RISK TRIAL

HIGH PROFILE TRIAL

MONEY ESCORTS

PERSONAL JUDICIAL SECURITY

MEDIA

COURT SECURITY ASSESSMENT

Location: _____

Prepared by: _____

Date: _____

TABLE OF CONTENTS

Individuals Interviewed	Page 2
Physical Security	Page 3
Personnel	Page 23
Equipment	Page 26
Operations	Page 28
Documentation	Page 40
Conclusions and Recommendations	Page 43

INDIVIDUALS INTERVIEWED

PHYSICAL SECURITY

- **GROUND**

- **Perimeter**

- 1) Is the perimeter clearly defined by a fence, wall or other type of physical barrier?
- 2) If so, describe the barrier and its condition.
- 3) Does the barrier limit or control vehicle or pedestrian access to the grounds?
- 4) Are there gates?
- 5) How do the gates operate?

- **LIGHTING**

- **Building (External)**

- 1) Are all entrances and exits well lit?

2) Are the lights on all night?

3) Are the lights automatically or manually controlled?

a) If manually, who is responsible?

4) Is there an auxiliary power source?

■ **Parking & Grounds**

1) Are all parking areas and walkways well lit?

2) Are the lights on all night?

3) Are the lights automatically or manually controlled?

a) If manually, who is responsible?

4) Is there an auxiliary power source?

- **PARKING**

- **Judicial**

- 1) Is there a separate area for judicial parking?
- 2) How is access controlled?
- 3) Is the area enclosed?
- 4) Is it identified as judicial parking?
- 5) Is this area monitored by CCTV?
- 6) Is there direct access into secure area of facility?

- **Employee**

- 1) Is there a separate area for employee parking?
- 2) If so, how is access controlled?

3) Is the area identified as employee parking?

4) Is it monitored by CCTV?

▪ **Public**

1) Is access to public parking controlled?

2) If necessary, could egress be sealed off?

3) Is the area monitored by CCTV or patrol?

● **LANDSCAPING**

1) Does landscaping provide places for hiding?

2) Are there foundation plantings which could be used to hide items including explosive devices?

BUILDING

- **DOORS, WINDOWS, OTHER OPENINGS**

- 1) What type of door and locks are used for external access points?
- 2) Are external doors alarmed?
- 3) Where are the hinges located on external doors?
- 4) Do emergency exit doors have outside handles?
- 5) Are there windows that are accessible from the outside that are operable?
 - a) If so, how are they secured?
- 6) What type of glass is used on windows?

7) Is the roof accessible externally?

a) If so, are there entrances into the building on the roof?

8) Is internal access to the roof controlled?

9) Are openings to the building such as tunnels, utility and sewer manholes, culverts, service ports properly controlled?

● **ACCESS CONTROL**

1) What type of access control is in place?

2) If keys are used, is there a key control system?

3) Who is responsible for the key control system?

4) Are master keys strictly controlled?

5) How are lost or non-surrendered keys handled?

- 6) Who can authorize additional keys to be made?
- 7) Are keys signed for and collected when no longer needed?
- 8) If access cards are used, are they swipe cards or proximity cards?
- 9) Is there any other electronic access control used, such as bio-metric?
- 10) What areas are controlled by electronic access?
- 11) Is the system usage recorded?
 - a) If so, how long are records kept?
- 12) Who controls the system?
- 13) Are cards signed for?

- **LOADING DOCK**

- 1) Is there a loading dock?
- 2) Is access to the loading dock controlled?
- 3) Are all deliveries made to the loading dock?
- 4) Is there an x-ray machine and magnetometer located on the loading dock?
- 5) Is there an officer assigned to the loading dock?
- 6) Are individuals making deliveries through the loading dock entering the facility?
 - a) If so, are they screened and identified?
- 7) Is this area monitored by CCTV?

- **CEILINGS & WALLS**

1) Do all walls extend to the ceiling where they separate private from public circulation?

2) Are drop or removable ceilings used?

a) If so, in what areas?

- **EMERGENCY POWER SYSTEM**

1) How frequent are power outages?

2) Is there an auxiliary power system?

3) What operates when the facility is operating under auxiliary power?

- **ALARMS**

1) Is there an intrusion alarm system?

2) Is the system tested periodically?

3) Where does the system terminate?

4) Are records of alarms maintained?

5) Is there a duress alarm system?

6) Where are the activators located?

7) Where do the alarms terminate?

● **SAFES & VAULTS**

1) How many safes and vaults are there?

2) What are they used for?

3) Are any of the safes alarmed?

4) Do any of them have a fire suppression system?

5) Are they key or combination locks?

6) How is access to safes controlled?

● **FIRE PROTECTION**

1) Does the facility comply with fire codes?

2) Has the facility been inspected by the Fire Marshal?

a) If so, when?

3) Is there a fire alarm system?

a) Where does it terminate?

4) Are there smoke and/or heat detectors?

5) Is there a sprinkler system?

6) Are there fire extinguishers?

a) Are they inspected and certified?

7) Are there emergency hoses?

● **UTILITY CONTROL POINTS**

1) Are utility access points locked when not in use?

2) If there is natural gas, is the connection to the building accessible?

3) Are air intake vents accessible?

● **ATTICS, BASEMENTS, CRAWL SPACES & ROOF**

1) Are doors to these areas locked when not in use?

● **ELEVATORS**

1) Are there private elevators for judges and staff?

- 2) Are there separate prisoner elevators?
- 3) Are prisoner elevators key operated?
- 4) Do prisoner elevators have bars to separate prisoners from officers?
- 5) Do prisoner elevators have CCTV and/or alarms?
- 6) Do elevators have emergency telephones?

● **STORAGE AREAS**

- 1) Are there any areas in which weapons, ammunition, chemical weapons are stored?
- 2) If so, how is access controlled?
- 3) Is an access log maintained?
- 4) What type of construction was used for this area?

- 5) Are there alarm, fire detection and sprinkler systems in this area?
- 6) Are there record storage areas?
- 7) Do these areas have fire detection and fire suppression systems?
- 8) Is access to these areas controlled?

● **COMMUNICATIONS**

- 1) What type of communication systems are available?

Telephone?

Hand-held Radio?

Public Address System?

Cell Phones?

- 2) Who controls the public address system?

- 3) How are radios deployed?

4) Can radios interface with other law enforcement agencies?

5) What capabilities does the telephone system have?

● **PUBLIC AREAS**

1) Are public waiting rooms adequate in size?

2) Are public waiting rooms in close proximity to courtrooms?

3) Are public waiting rooms under observation by an officer or CCTV?

4) Are there security/information posts in public areas?

5) Are entrances to public restrooms under observation by an officer or CCTV?

6) Is there adequate signage to assist the public?

- **HOLDING CELLS**

- 1) Is there a central detention area?
- 2) Are there holding cells adjacent to the courtrooms?
- 3) Are there facilities for attorney-client conferences?
- 4) Does each holding cell contain a toilet/sink unit?
- 5) Can cells be monitored from a central location?

- **OFFICE AREAS**

- 1) Is public access allowed in office areas?
 - a) If so, how it is controlled?
- 2) Are there cashier windows?

- 3) Do cashier windows have security features such as glass or bars separating public from private areas?
- 4) If money is handled, are there secure facilities to protect the money?
- 5) If there is a vault, are appropriate procedures in place to ensure the integrity of handling of money?

● **COURTROOMS**

- 1) Do courtrooms have railings separating the spectators from the well of the courtroom?
- 2) Does the courtroom allow for easy exit by the judge if there is an emergency?
- 3) Is the bench lined with ballistic material?
- 4) Does the courtroom allow for easy egress by the jury?
- 5) Is the jury separated from the spectator area of the courtroom?

6) Are there duress alarms in the courtroom?

a) If so, what is their location?

7) Are there CCTV cameras located in the courtroom?

8) Can audio activity be monitored from outside the courtroom?

9) Can all doors to the courtroom be locked?

10) Is there direct access into the courtroom from holding cells?

11) Can defendants receive video and/or audio feeds in holding cells from the courtroom?

12) Are counsel tables affixed to the floor?

● **JUDGES CHAMBERS**

1) Are judges' chambers located in private areas?

- 2) How is access to chambers controlled?
- 3) Is there dual egress from the judges' offices?
- 4) Are there duress alarms located in chambers?
- 5) Do chambers have operable windows?
- 6) Can individuals see in windows in chambers?
- 7) Who has keys to chambers?

● **WITNESS WAITING ROOMS**

- 1) Where are witness waiting rooms located?
- 2) Is access controlled?

- **ATTORNEY-CLIENT CONFERENCE ROOMS**

- 1) Where are attorney-client rooms located?

- 2) Is access controlled?

- **JURY ASSEMBLY AREA**

- 1) Is access limited to jurors?

- 2) How is access controlled?

- **JURY DELIBERATION ROOMS**

- 1) Where are jury deliberation rooms located?

- 2) Does each room contain a restroom?

- 3) Can individuals outside the room hear what jurors are saying?

- **CIRCULATION SYSTEMS**

- 1) Are there public, private and prisoner circulations systems?
- 2) How is access to private and prisoner systems controlled?

- **SECURITY OPERATIONS OFFICES**

- 1) Where are they Security Operations Offices located?
- 2) Does the public have access to the offices?
- 3) Do higher ranking supervisors have private offices?

PERSONNEL

- **ORGANIZATION CHART**

- 1) Does the organization chart clearly show the chain of command?

- **NUMBER OF PERSONNEL**

- 1) What is the determining factor as to the number of personnel?

- 2) How are the number of supervisory personnel determined?

- **DEPLOYMENT OF PERSONNEL**

- 1) Is there a published deployment schedule?

- **TRAINING**

- 1) Is there mandatory recruit training?
- 2) What does recruit training consist of?
- 3) Is there a mandated in-service training program?
- 4) What does the in-service training consist of?
- 5) Do individuals attend outside training?

- **SPECIAL UNITS**

- 1) Is there a unit to deal with judicial threats?

2) Is there a training unit?

3) Is there a medical response unit?

4) Are there any other special units?

● **APPEARANCE**

1) Does the uniform present a professional appearance?

2) Do the officers present a professional appearance?

● **SERVICE TO THE PUBLIC**

1) Does the organization emphasize public service?

2) Are there any programs which educate the public about the courts?

EQUIPMENT

[illegible]

EQUIPMENT

[illegible]

OPERATIONS

- **COURTROOM**

- 1) Do officers have specific posts?
- 2) Who determines what those posts are?
- 3) Who is in charge of the operations in each courtroom?
- 4) What type of communications are available in each courtroom?
- 5) Who is responsible for evidence while it is in the courtroom?
- 6) Are there specific procedures relative to other law enforcement personnel who may be in the courtroom?
- 7) Are courtrooms searched prior to being opened?
- 8) Do the officers assume any responsibility relative to decorum?

9) Are there specific rules governing the media while they are in the courtroom?

10) Does each person know their role if there is an incident?

11) Are courtrooms monitored by CCTV?

● **SCREENING**

1) Under whose authority is screening done?

2) Who is subject to be screened?

3) If there are exceptions, who has the authority to grant exceptions?

4) If there are exceptions, how are they handled?

5) Are logs maintained for such things as law enforcement personnel, visitors, individuals in the facility during off hours?

- 6) How are magnetometers and x-ray machines configured?
- 7) What are the traffic flows and cueing -up arrangements?
- 8) What constitutes contraband?
- 9) How is contraband handled?
- 10) If vouchered, what are procedures?
- 11) What is the policy relative to firearms coming into the facility?
- 12) Are there procedures for vouchering firearms?
- 13) Do screening stations include ballistic material?
- 14) Who is responsible for calibrating magnetometers?

- 15) Are there set procedures for the screening process?
- 16) Are there procedures for handling individuals in wheelchairs, children in carriages and individuals with pacemakers?
- 17) What is the staffing for magnetometer posts?
- 18) Are there on-site supervisors for screening operations?
- 19) Are assignments to screening operations permanent assignments?
- 20) Are there significant complaints about officers assigned to screening operations?
- 21) Are screening operations monitored by CCTV?

● **EXTERIOR**

- 1) Do court security personnel have a responsibility outside the court facility?
- 2) If so, what is the nature of their responsibility?

3) Is there exterior security operations during non-business hours?

4) Is the exterior of the facility monitored by CCTV?

● **PUBLIC AREAS**

1) Are there security posts in the public areas of the facilities?

2) What is the nature of security operations in the public areas?

3) Are public areas monitored by CCTV?

● **PRISONER**

1) How are prisoners delivered to the courthouse?

2) Who is responsible for holding prisoners while in the court facility?

3) How is prisoner movement within the facility handled?

- 4) Are there set policies relative to prisoner property?
- 5) How are attorney/client conferences handled while in the facility?
- 6) What is the policy relative to cuffing prisoners?
- 7) What is the policy relative to shackling?
- 8) What is the procedure on remands?
- 9) Is there a set policy on the ratio of officers to prisoners during movements?
- 10) Is there a set policy on officer supervision of prisoners while they are in holding cells?
- 11) Is there a set policy regarding transfer of custody to include property?
- 12) Is there a practice relative to evaluating prisoners as to suicide risks, etc.?

- 13) Is there a policy relative to segregating prisoners?
- 14) Is there a policy relative to the handling of disabled or handicapped prisoners?
- 15) Is there a policy relative to what to do if a prisoner has a child with them?
- 16) Is there a policy relative to what to do if a prisoner needs medical treatment?
- 17) Is there a policy relative to juveniles?
- 18) Is there a policy relative to prisoners being released from custody at the courthouse?

● **SPECIAL OPERATIONS**

- 1) Do the courts have trained medical response personnel?
- 2) Is there a special unit to respond to threats against the judiciary?
- 3) Is there a canine unit?

4) Is there a special weapons unit?

● **EMERGENCY OPERATIONS**

1) Is there a designated critical incident manager for the facility?

2) Is there a designated alternate and chain of command for the critical incident manager?

3) Has a bomb threat checklist been distributed?

4) Is it clearly established who makes the decision to evacuate?

5) Is search in place one of the options available?

6) Do non-sworn individuals know their role in the case of a bomb threat?

7) Have search procedures been established?

8) Is the Emergency Services Unit familiar with the facility?

- 9) If the facility fire alarm system does not automatically alert the fire department, is it clearly established who is to call?
- 10) Is it established who can give the “all clear” after a fire alarm?
- 11) Do officers have a clear understanding of their role in a hostage situation?
- 12) Has liaison been made with the Hostage Negotiating Team?
- 13) Are there certified emergency medical personnel in the facility?
- 14) Is there an established procedure to deliver supplies and equipment to the scene?
- 15) Is it established who is to call for an ambulance, if necessary?
- 16) Is someone designated to ensure supplies and equipment are maintained?

17) Are evacuation drills done?

a) If so, are they evaluated and documented?

18) Are the distances from the building that people should be evacuated to clearly established?

19) Do evacuation plans include provisions for the evacuation of judges, prisoners and jurors?

20) Do the evacuation plans include provisions for a Command Post and Alternate Command Post?

21) Has it been clearly established whether demonstrations can take place inside the facility?

22) Are permits required for demonstrations?

23) Is there a policy on the distribution of written material inside the facility?

24) Is there a policy on the hanging of signs and/or posters inside and outside the facility?

25) Is there a policy on the use of court facilities by outside groups?

26) Have officers been trained in crowd control tactics?

● **ARRESTS**

1) Is there a clear policy on arrests?

2) Are arrest procedures known?

3) Are officers able to issue appearance tickets?

● **ADMINISTRATION**

1) Is there adequate supervision for operations?

2) Are supervisors visible?

3) Do supervisors set the proper tone for officers?

4) Is there an established procedure for addressing complaints against officers?

5) Are officers evaluated?

6) Do the rank and file have an opportunity to have input into procedures?

● **COMMUNICATIONS**

1) Is there an adequate communication system?

2) Are there provisions for inter-agency communications?

3) What are the various communication options?

● **JURY SUPERVISION**

1) Are there established procedures for the supervision of jurors?

2) Is juror information collected by officers supervising sworn jurors?

3) Is there a policy if an officer knows a juror?

- 4) Are juries ever sequestered?
- 5) What is the policy on telephone calls for sequestered jurors?
- 6) Is there a policy if a sequestered juror should require medical treatment?
- 7) Is there a plan if a sequestered jury must be evacuated from a hotel?
- 8) Does the crew supervising a sequestered jury have emergency contact numbers?

- **OFFICE AREAS**

- 1) Do office areas have uncontrolled public access?
- 2) Have office personnel been instructed what to do in emergency situations?

DOCUMENTATION

- **RULES AND PROCEDURES MANUAL**

- 1) Is there a Rules and Procedures Manual?

2) Is each officer issued a Rules & Procedures Manual?

● **STANDARD OPERATING PROCEDURES**

1) Are there Standard Operating Procedures?

2) Is each officer issued SOPs?

3) Are the SOPs updated?

4) Do the SOPs cover all aspects of operations?

● **EVACUATION PLANS**

1) Are there evacuation plans for all facilities?

2) Are personnel familiar with the plans?

3) Are drills conducted?

- 4) Are the plans appropriately disseminated?
- 5) Have plans been approved by the Fire Marshal?
- 6) Do the plans include floor plans of the facilities?
- 7) Do the plans include alternate sites for judges and court operations?

● **INCIDENT REPORTS**

- 1) Are there formal reports for recording various types of incidents?
- 2) Are reports reviewed by supervisory personnel?

CONCLUSIONS AND RECOMMENDATIONS

APPENDIX D

BOMB THREAT REPORT FORM¹

INSTRUCTIONS: BE CALM. BE COURTEOUS. LISTEN, DO NOT INTERRUPT THE CALLER. NOTIFY SUPERVISOR/SECURITY OFFICER BY PREARRANGED SIGNAL WHILE CALLER IS ON LINE.

Date: _____ Time: _____

Exact Words of Person Placing Call:

QUESTIONS TO ASK:

1. When is the bomb going to explode? _____
2. Where is the bomb right now? _____
3. What kind of bomb is it? _____
4. What does it look like? _____
5. Why did you place the bomb? _____

TRY TO DETERMINE THE FOLLOWING (CIRCLE AS APPROPRIATE)

Caller's Identity: Male Female Adult Juvenile Age _____ years

Voice: Loud Soft High Pitch Deep Raspy Pleasant Intoxicated

Other _____

Accent: Local Not Local Foreign Region

Speech: Fast Slow Distinct Distorted Stutter Nasal Slurred

Lisp Other _____

Language: Excellent Good Fair Poor Foul Other _____

Manner: Calm Angry Rational Irrational Coherent Incoherent

Deliberate Emotional Righteous Laughing Intoxicated

Background Noises: Office Machines Factory Machines Bedlam Trains

Animals Music Quiet Voices Mixed Airplanes Street

Traffic Party Atmosphere

ADDITIONAL

INFORMATION: _____

ACTION TO TAKE IMMEDIATELY AFTER CALL: Notify your supervisor/security officer as instructed. Talk to no one other than instructed by your supervisor/security officer.

RECEIVING TELEPHONE NUMBER: _____

PERSON RECEIVING CALL: _____

¹ San Diego County Sheriff's Department, *Manual of Policies and Procedures* (San Diego, California: 1975), No. 3.3.9, p. 2.



National Institute of Justice

Research Preview

Jeremy Travis, Director

June 1997

Court Security and the Transportation of Prisoners

Summary of a Research Study by the National Sheriffs' Association

The sharp rise of violence in court settings—from minor disturbances to murder—has prompted a reexamination of safeguards for the judicial process and personnel and of the transportation of prisoners to and from court. The National Institute of Justice (NIJ) sponsored an assessment by the National Sheriffs' Association (NSA) of the current state of the art in court security and the transportation of prisoners.

The study's three surveys found that the safety of personnel transporting and monitoring prisoners in the courtroom is the most pressing concern. Possible responses include improving training through more intense classroom instruction and field training for high-risk situations, providing personnel with appropriate equipment, enhancing facilities' structural features, and establishing policies and procedures for courtroom security and for safe prisoner transport—on the ground and in the air. The assessment offers specific suggestions for agencies to consider when evaluating their individual programs.

Study method

Information was gathered from interviews and questionnaires administered to court security, probation, parole, and sheriffs' personnel nationwide; a review of existing research literature and reports of some of the violent incidents that occurred in courts over the past two decades; and input from the Project Advisory Board, Staff Review Committee, practitioners, experts in the field, and other criminal justice organizations.

Personnel education and training

The majority of court security and prisoner transport personnel are 40- to 50-year-old males who attended college for at least 1 or 2 years and are very satisfied with their jobs. A majority have completed a training program in court security, prisoner transportation, or serving of civil or criminal process.

However, many felt they were not fully prepared to meet new and emerging challenges. Fewer than half the re-

sponding agencies provide training in vehicle operation, which is a key area for liability actions. Also, fewer than half the agencies instruct officers in the proper application of commonly used restraining devices (e.g., handcuffs, straps, leg irons). A vehicle operation training curriculum could include commercial driver's license requirements; driver's pursuit and defensive training; liability issues; care, custody, control, and supervision procedures; driver and escort officer/deputy responsibilities; and use of specialized equipment.

In addition, although they rarely perform routine maintenance tasks, over half the respondents said they inspect some security equipment (e.g., vehicles, doors) and conduct security checks inside and outside courthouses. Fewer than half, however, inspect equipment such as scanning devices, alarms, and cameras.

Respondents said they need more instruction in legal liabilities; legal responsibilities of supervision; firearms; court functions, duties, and security; serving of civil or criminal process; and transporting prisoners both on the ground (e.g., in an automobile, bus, or van) and in the air. They also felt they needed more education about vicarious liability; possible areas for suits include failure to train or direct and negligence in supervision, entrustment, assignment, hiring, and retention.

The study suggests that basic court security and prisoner transport training programs should provide a minimum of 80 hours of classroom instruction over a 4- to 6-week period. Personnel should also be certified in certain key areas such as the use of electronic nonlethal equipment (e.g., stun, laser, and taser guns and stun belts) and methods of applying physical force to control defendants in high-risk situations.

All trainees should pass examinations to demonstrate they have adequate knowledge and skills before they are assigned to security or prisoner transport duties. The Federal Aviation Administration (FAA) requires personnel transporting prisoners to pass a certified 2-hour block of training.

Court facility security

Court security staff comprise sworn and unsworn personnel (e.g., bailiffs, private-sector employees, and Federal and State Department of Corrections personnel).

Fewer than half the court agencies and sheriffs' offices said they put a high priority on controlling access into court and judicial facilities—e.g., patrolling exterior perimeters, scanning mail and packages, and supervising elevator use. Probation and parole personnel think metal detectors should be used more often outside courtrooms.

The study suggests that the underlying principle of court security should be maintaining a physical security system that does not interfere with the activities of the court.

A key aspect of security involves providing physical mechanisms for safe passage inside and outside court facilities. Consideration should be given to employing structural features and controlled access devices, in compliance with the Americans with Disabilities Act of 1990, such as the following:

- Adequate lighting and proper landscaping around parking areas, walkways, and at points of access where visual recognition is necessary.
- Barriers to prohibit forcible entry by vehicles or pedestrians.
- Bullet-resistant glazing on windows in all areas of sight exposure as well as shatter-resistant film between layers of glass and sensor devices on ground-floor windows.
- Designated parking areas for judges and selected court employees, prisoner transport, and service-related vehicles.
- Mechanisms on perimeter doors that can detect unauthorized entry.
- Controlled access to building facilities through separate, electronically monitored entrances for the general public, judges, court personnel, and service personnel.
- Distinct structural circulation systems within the courthouse to limit access for visitors, prisoners, and outside service personnel and to provide secure passage for judges, juries, and court staff (e.g., restricted elevators for different users and centralized holding areas for prisoners).

Policies and procedures regarding use of these mechanisms need to be continually monitored and updated. Each hearing and trial should be assessed to determine the correct level of security needed. This assessment could prepare security officers/deputies for any disruptions that may

occur and could keep costs down by increasing staff only when appropriate. A balance should be struck between protecting all who enter the court and permitting normal operations.

Transportation of prisoners

The majority of probation and parole agents surveyed believe uniformed officers (e.g. deputy sheriffs/officers) should transport prisoners, even though most of the respondents have been required as part of their official duties to do the transporting. Although transporting male adults, female adults, male juveniles, and female juveniles requires different guidelines, fewer than half the respondents have ever received special or refresher training in prisoner transportation. Survey respondents indicated that most agencies do not possess vehicles specially equipped to transport prisoners. In addition, over half the agencies do not allow agents to perform gender-appropriate strip searches.

Rules or procedures exist in several jurisdictions governing the transportation of prisoners, but there are no national regulations (except those issued by the FAA). The study suggests that the first step should be implementation of a “dangerousness” classification for prisoners being transported so security officers can implement the proper levels of care, custody, control, and supervision. Other suggestions concern providing handheld radios for all transport personnel and establishing a statewide or regional radio frequency so help can be summoned quickly in an emergency.

All prisoners should be monitored continuously in case medical emergencies arise. If such an emergency does occur during transport, officers/deputies should be prepared to take appropriate action and know how to handle patients with infectious diseases. An agency's medical unit should inform transporting officers/deputies if a prisoner has a communicable disease and provide guidelines that follow those mandated by the U.S. Occupational Safety and Health Administration and the Centers for Disease Control and Prevention.

Conclusion

A risk assessment should be an integral part of a comprehensive survey of courtroom security and the transportation of prisoners to determine security vulnerabilities and equipment and training needs. Even the most sophisticated equipment is only a supportive tool used by trained personnel as part of a well-prepared plan to administer justice in a danger-free environment.

This Research Preview highlights a study, supported under NIJ grant 94-IJ-CX-0005, by the National Sheriffs' Association. The executive summary and full report, *Court Security and the Transportation of Prisoners: A National Study*, written by NSA Executive Director Charles B. Meeks, Project Director A.N. Moser, Jr., and Senior Research Consultant Betty B. Bosarge, are available through interlibrary loan or copy satisfaction from the National Criminal Justice Reference Service at 800-851-3420, or through e-mail at askncjrs@ncjrs.org. Ask for NCJ 161710 (executive summary), NCJ 161701 (volume one), and NCJ 161702 (volume two).

FS 000165

Points of view in this document do not necessarily represent the official position or policies of the U.S. Department of Justice.

Selected NIJ Publications About Courts, Crime Prevention Through Environmental Design, and Victimization and Violence

Listed below are some NIJ publications and videos related to issues of courts, Crime Prevention Through Environmental Design, and victimization and violence. These products are free, except as indicated, and can be obtained from the National Criminal Justice Reference Service (NCJRS): telephone 800-851-3420, e-mail askncjrs@ncjrs.org, or write NCJRS, Box 6000, Rockville, MD 20849-6000.

These documents also can be downloaded through the NCJRS Bulletin Board System or at the NCJRS Anonymous FTP site in ASCII or graphic formats. They can be viewed online at the Justice Information Center World Wide Web site. Call NCJRS for more information.

Please note that when free publications are out of stock, they are available as photocopies or through interlibrary loan.

Courts

Anderson, David C., *In New York City, a "Community Court" and a New Legal Culture*, Program Focus, 1996, NCJ 158613.

The Drug Court Movement, Update, 1995, FS 000093.

Finn, Peter, and Andrea K. Newlyn, *Miami's "Drug Court": A Different Approach*, Program Focus, 1996, NCJ 142412.

Whitcomb, Debra, and Mark Hardin, *Coordinating Criminal and Juvenile Court Proceedings in Child Maltreatment Cases*, Research Preview, 1996, FS 000157.

Crime Prevention Through Environmental Design

Fleissner, Dan, and Fred Heinzelmann, Ph.D., *Crime Prevention Through Environmental Design and Community Policing*, Research in Action, 1996, NCJ 157308.

Gordon, Corey L., and William Brill, *The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability*, Research in Brief, 1996, NCJ 157309.

Smith, Mary S., *Crime Prevention Through Environmental Design in Parking Facilities*, Research in Brief, 1996, NCJ 157310.

Taylor, Ralph B., and Adele V. Harrell, *Physical Environment and Crime*, Research Report, 1996, NCJ 157311.

Victimization and Violence

The Extent and Costs of Crime Victimization: A New Look, Research Preview, 1996, FS 000131.

Fein, Robert A., Ph.D., Bryan Vossekuil, and Gwen A. Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, Research in Action, 1995, NCJ 155000.

Finn, Peter, and Kerry Murphy Healey, *Preventing Gang- and Drug-Related Witness Intimidation*, Issues and Practices, 1996, NCJ 163067.

Healey, Kerry Murphy, *Victim and Witness Intimidation: New Developments and Emerging Responses*, Research in Action, 1995, NCJ 156555.

Kellermann, Arthur L., M.D., M.P.H., *Understanding and Preventing Violence: A Public Health Perspective*, VHS videotape, 1995, NCJ 152238, U.S. \$19, Canada and other foreign countries \$24. A summary of the presentation is available as a Research in Progress Preview, 1996, FS 000141.

Roth, Jeffrey A., and Mark H. Moore, *Reducing Violent Crimes and Intentional Injuries*, Research in Action, 1995, NCJ 156089.

State and Local Responses to Terrorism, Update, 1995, FS 000092.

Quick Access to NIJ Publication News

For news about NIJ's most recent publications, including solicitations for grant applications, subscribe to JUSTINFO, the bimonthly newsletter sent to you via e-mail. Here's how:

- Send an e-mail to listproc@ncjrs.org
- Leave the subject line blank
- Type subscribe justinfo your name
(e.g., subscribe justinfo Jane Doe) in the body of the message

Or check out the "What's New" section at the Justice Information Center homepage:
<http://www.ncjrs.org>

U.S. Department of Justice

Office of Justice Programs

National Institute of Justice

Washington, DC 20531

Official Business

Penalty for Private Use \$300

BULK RATE
POSTAGE & FEES PAID
DOJ/NIJ
Permit No. G-91



Courthouse security photo courtesy DuPage County, Ill., Sheriff's Office

Court Security By Design

By Michael A. Griebel, SVP, Healy, Bender & Associates, Inc.,
Hon. Fred A. Geiger, Judge, Second Court of Appeals, State of Illinois,
and Sheriff John E. Zaruba, DuPage County, Ill.

Court facilities should provide a safe and secure environment for the staff, judges, jurors, general public and those held awaiting trial. Court security has a simple but critical purpose—to protect the integrity of court processes and proceedings. As the late Chief Justice Warren Burger and former U.S. Attorney General William French Smith once declared, “If we cannot ensure the safety of all participants in the judicial process, we cannot maintain the integrity of the system, we cannot—in sum—establish ‘justice,’ as mandated in the preamble to the Constitution of the United States.”

This article outlines some basic design concepts and requirements for a secure modern court facility. Modern court facilities make use of zoned protection, with intensifying areas of security defined at or beyond the site perimeter as one moves to the interior of the building. In all cases, court facilities should be designed to allow increases in security in response to specific or elevated threats. Conversely, it should be possible to reduce the security when warranted. Effective security only can be provided through a combined approach that integrates good policy, procedure, and operations; appropriate architecture; and effective security systems.

Achieving effective court security requires the input and cooperation of those using the courthouse, those responsible for court security, and those architects, engineers and specialists charged with coming up with a design that is appropriate for security. Each building system and element should be designed with an eye toward mitigating risk, reducing casualties and property damage, and protecting against the loss of critical functions. Security should be considered in all design decisions, from selection of furniture to placement of trash receptacles to designing redundant electrical systems.

Since most courthouses in the U.S. are not new, the criteria should be seen as objectives, and they should be used as a benchmark when planning security upgrades and improvements.

Primary Goals

Security objectives to be met in new or renovated courthouses today include:

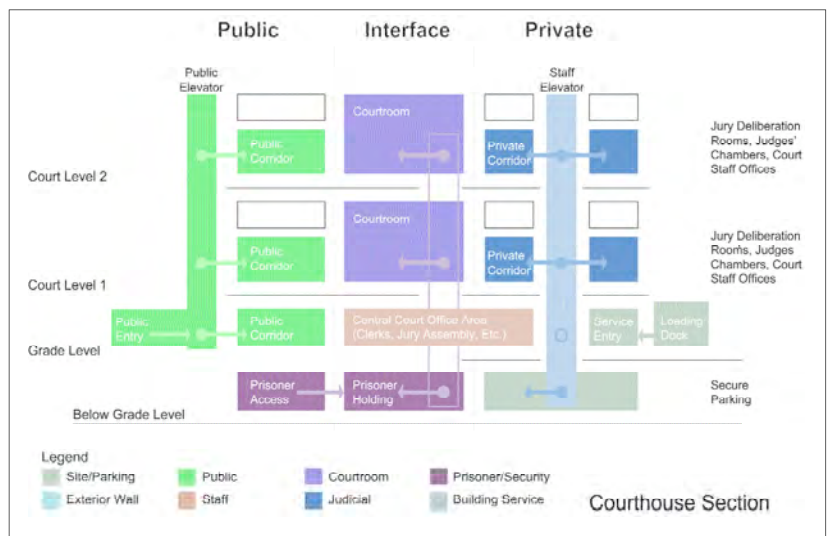
- detection of actual or potential threats, and eliminating any opportunity for the threat insofar as possible
- detection of breaches of security
- delaying the progression of an incident that a perpetrator may need to pull off quickly for it to be effective
- halting and controlling the event after it has started
- minimizing or eliminating damage arising from such incidents.

The Basic Concept

Courthouse facilities should be organized into four zones that group individuals coming to the courthouse based on their function and separate them until they meet in the courtroom. The four zones are the “public zone,” the “private zone,” the “prisoner zone” and the “interface zone.” Access between the four zones should be controlled by passage through controlled (and often-monitored) doors. Depending on security requirements, door locks may be released by keys, keying numbers into touch pads, use of card-access readers, electronic strikes, or they may be remotely controlled from a central security station. Admission to restricted areas should be discouraged by signage and locked doors, and motion-detection sensors may be used to activate audio warnings to encourage non-authorized persons to keep their distance from designated areas. The four zones should be served by discrete systems for public, private and prisoner circulation. In addition, freight service should provide direct and easy access throughout the courthouse to and from the building support/service areas and the loading dock.

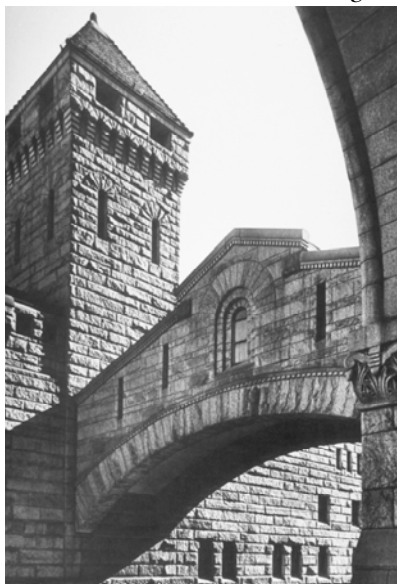
These principles of separation for different users have evolved only slightly from early governmental structures dating back more than

Continues page 42



a century. For example, in Pittsburgh, the overhead "Bridge of Sighs" spanned the street between the 1888 Allegheny County Jail and Courthouse, providing a direct link between the facilities for in-custody prisoner movement.

Unfortunately many courthouses designed in the U.S. between 1900 and 1960 ignored



Allegheny County Jail and Courthouse linked by overhead bridge

these basic concepts. Importantly, the American Bar Association published the 1973 monograph "The American Courthouse,"² and the basic principles of separation of spaces and circulation systems in court facilities have been reaffirmed and restated in a number of state and national publications and guidelines released over the past 30 years.³

Public Zone

The public zone of the courthouse contains offices and support areas serving the public. Located throughout a courthouse, public areas include the main entry to the building, the main circulation paths to courtrooms and the reception areas of all court-related offices. Such areas include public lobbies, public restrooms, fine-collection areas, courtrooms, certain public service and security functions, and other public service areas and office areas.

Public access to the court building should be provided through a single primary public entry designed to handle peak volumes of people without compromising procedure. The screened entry point should be located far enough inside the

weather vestibule to allow for queuing. All persons using the public entrance should be required to pass through a metal detector and x-ray package screening station. All staff except judges should be required to pass through the public entrance as well, and all staff (including judges who elect to enter through the public entrance) should be required to pass through the metal detector or weapon-detection system.

The public entry, hallways, elevators, escalators (if provided) and stairs must be capable of being supervised or monitored by direct observation by staff at the security station and by closed-circuit video equipment at the building control center. Public circulation on courtroom floors should be limited to a public corridor system providing access to courtrooms and waiting areas. All public areas should be properly illuminated and clearly identified with good signage, including directories.

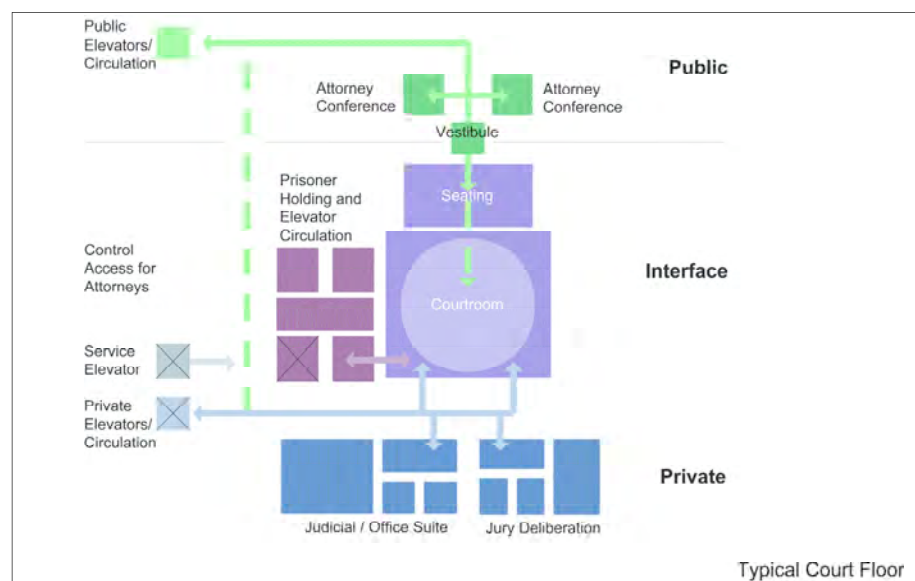
Public areas should be separated from employee offices by walls or counters. Receptionist areas and cashier stations should be designed with appropriate separation from waiting rooms and public areas. Public access to clerk staff areas should be limited to counter access or easily supervised public desk locations. Areas of the courthouse and departments with lower numbers of public visitors typically should be located in areas more remote from the public entry to limit unintentional movement of the general public into restricted areas.

Private Zone

The private zone includes spaces for judges, jurors, staff and authorized users. Private zone areas are usually treated as restricted access areas (staff and invited visitor access only). Private zone circulation should enable judges, court personnel and other authorized personnel to enter a private circulation system (hallways, elevators, stairs) through a restricted entrance.

Private circulation should allow judges, staff, authorized personnel and impaneled jurors to proceed between jury-deliberation areas, chambers and judicial work areas, all courtrooms and all hearing rooms without encountering either the general public or prisoners. Proper screening of individuals is crucial in this area. Philosophically access to this area should be similar to the access control of a law office, where staff are assigned to monitor and supervise access into the offices of the judges and judicial support staff. The judicial entrance to the facility should be equipped with card access or other device to unlock the door. The door should be alarmed against both forced entry and failure of the door to close properly. The entrance and door should be monitored by a CCVE system.

Direct, secure and easy access through private circulation to all courtrooms should include restricted-use, handicapped-accessible elevators to support the vertical movement of judicial officers and court staff independent from the public. This system should extend from the lowest building level and be capable of stopping at all court floors of the new facility. Restricted circula-



tion on courtroom floors consists of a corridor system that is separate from the public circulation system and the in-custody movement system. Similarly, restricted circulation on court support and court-related office floors should be separate from public circulation. No visitor should be allowed unescorted access into the private circulation system. In the event that a judge has a visitor, the staff should announce the visitor to the judge. If access is permitted, staff should escort the visitor to the judge's chambers.

Prisoner Zone

The prisoner zone includes spaces for movement and short-term detention of persons in custody. Ideally each courtroom that is planned to accommodate appearances or trials involving in-custody defendants or parties should have direct access from the prisoner zone. All prisoner areas, including all elevators and corridors for secure prisoner circulation, should be visually and acoustically separated from the public, private and interface zones. Inmates being moved should never encounter jurors, judges, court staff or the public until they are brought into the courtroom.

The prisoner circulation, access and detention areas provided in the facility should be designed with appropriate security sallyport access and control points, as well as monitoring and control equipment. This sallyport entrance should provide vehicular and pedestrian access into the facility's detention/prisoner areas. Typically needed is a central holding and prisoner-distribution area to receive in-custody defendants and process them for transport to specific courtrooms. All designs should provide direct circulation from the vehicular sallyport area into a prisoner elevator or stair, and then to a secure corridor with central holding areas (typically located on a lower level of the facility), to prisoner elevator(s) and stair(s) providing direct circulation to smaller prisoner holding areas located directly between courtrooms. From these holding areas, prisoners will be moved directly into the litigation area, or "well," of the courtroom.

The holding cells should be designed to meet national and state standards for temporary holding facilities and should be equipped with duress alarms, modern communications equipment and closed-circuit video equipment for monitoring. Provisions should be made for separation (physical, visual and acoustic) for various classifica-

tions of in-custody defendants. It may be necessary to provide complete physical separation of several types of in-custody persons (for example, adult male, adult female, special cases).

A secure perimeter system should surround the central holding or cell block areas, the courtroom holding areas and other areas included in the prisoner system. All points of entry or egress through this perimeter should be controlled by sallyports with interlocked doors and monitored at the building control center. All walls, floors, ceiling systems, fenestration systems and penetrations should be designed to meet current design standards for short-term detention areas.

Interface Zone

The interface zone is where the attorneys and the public meet judges, court staff, jurors and those in custody—generally, the courtroom. These interface areas generally require the greatest care in location and design, as they are integral parts of each zoning system. These interface areas are typically the focus of the judicial proceedings and must therefore reflect the appropriate image of the justice system in a way that is not compromised by unduly obtrusive security measures.

Securing the courtroom requires proper design, sound operating procedures and

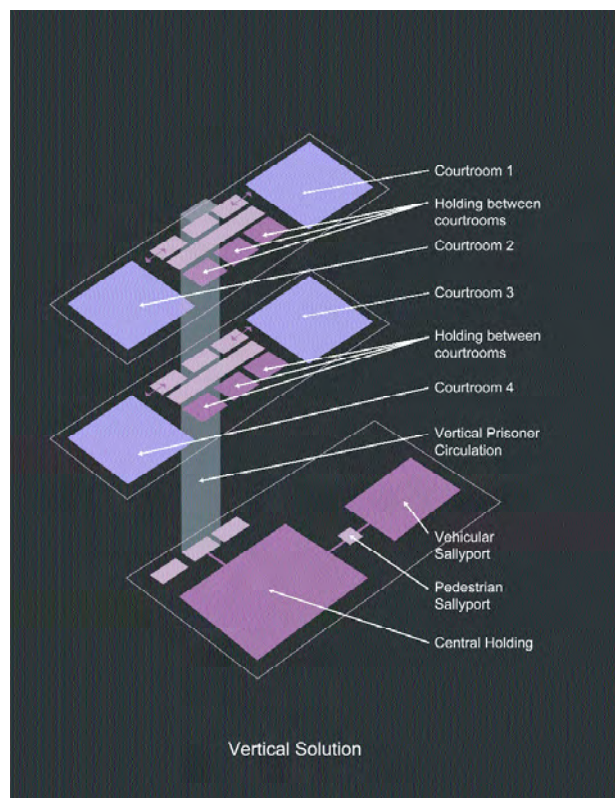
thorough staff training. Courtrooms should be designed to provide appropriate separation and unobstructed view between the judge, witnesses, parties and the public. It is essential to maintain proper separation and distance between the defendant and other courtroom participants. Bullet-resistant liners should be provided within the courtroom millwork personnel stations, including the witness box. Security glazing may be required to protect windows and doors. Duress alarms should be provided on the judge's bench and at the clerk's desk.

Movable furniture provided in courtrooms, hearing rooms and public areas of the courthouse should be heavy and difficult to grasp, lift and throw. If necessary, chairs, tables and other furniture may need to be fixed to the floor. There should also be a railing between the trial area and spectators so prisoners cannot reach the public.

Using CPTED Principles in Site and Building Design

Crime Prevention Through Environmental Design (CPTED) concepts stress three things particularly important in the design for security of the court building site and the public areas inside the building: "Natural access control; natural surveillance; territorial reinforcement."⁴ Access control and surveillance are primary architectural concerns. The concept behind access control is

to deny access to a crime target and to create a perception of risk in would-be offenders. Access control can involve use of staff, barriers (natural or artificial), and equipment (locks, cameras, detection equipment). Surveillance is a design concept directed primarily at keeping would-be intruders under observation. Surveillance strategies can involve staff (law enforcement patrol or presence), mechanical and electrical means (lighting, cameras) and natural means (windows, open sightlines). Territorial reinforcement involves designing sites and buildings in such a way that crime prevention flows naturally and routinely from the activities within and around the courthouse.



The CPTED concepts focus on “natural” barriers and systems, sometimes referred to as “passive” design solutions, and on “artificial” systems, sometimes referred to as “active” solutions that rely heavily upon electronics-based security equipment. The common thread that runs through all of the concepts is a primary emphasis on “naturalness.” The concepts are intended to support the things one would naturally do and to make it possible to do them better. Some strategies for integrating the concepts in courthouse planning and design include:⁵

- providing clear border definition of controlled space
- providing clearly marked transitional zones that indicate movement from public to semi-public to private space
- relocating gathering areas to locations with natural surveillance and access control, or to locations away from the view of would-be offenders
- redesigning the use of space to provide natural barriers to conflicting activities
- improving scheduling of space to allow for its effective use and clustering of activities as appropriate
- redesigning space to increase the perception—or reality—of natural surveillance
- overcoming distance and isolation through improved communications and design efficiencies.

Other Design Requirements

The primary security perimeter of a free-standing courthouse consists of the “building envelope” (exterior walls, windows/doors, roof and other openings). The security perimeter should be designed to restrict and delay unauthorized access and provide notification to security personnel if entry is attempted. Special attention should be given to all openings between the exterior and the walls or roof. Door and window controls should be properly planned, designed and installed for appropriate strength and reinforcing. Many courts require intrusion-detection systems with central monitoring capabilities.

Courthouses should be designed to provide appropriate security and protection during both periods of routine activity and times of emergency. Preparedness planning is a critical element when developing a courthouse’s security plan for any courthouse. At a minimum, secure “places of refuge” should be designed for both the judiciary and prisoners. In the event of an emergency, there should be a location in the facility for the judges to gather. Security staff can then determine if evacuation from the building is required and, if so, can provide protection as judges exit.

The building security center should be functional and efficient—in most cases, a monitoring and communications room, designed with access flooring (panel system). Natural light should be controlled to limit glare and veiled reflections and restrict ultraviolet light. Security posts should be integrated into the courthouse design yet should be visible and clearly identifiable.

Building-support spaces (mechanical, electrical rooms and other storage and support areas) should be treated as separate and controlled areas, and dedared and posted “off-limits” to everyone except authorized personnel. That is because these areas could be used as hiding places for contraband, persons and/or weapons. Therefore, these areas should be fitted with door closers and automatic locks to ensure that they are kept closed and locked.

Provision of fire- and burglar-resistant vaults or safes may be necessary in the facility for the storage of dangerous or valuable items,

exhibits and evidence. A separate burglar-resistant safe may be required for the storage of funds collected at child-support or fine-payment areas, in the clerk’s office and other areas. Motion detectors should be installed in any secure rooms that have breakable walls.

After-hours access to the courthouse should be provided only through doors that provide an identifying electronic record of the location, time and key (or card) used. After-hours access between the general court security perimeter, the staff security area and any in-custody security areas may be similarly recorded.

Because security systems are dependent on the building’s electrical supply, maintaining that supply is critical to maintaining building security. In large facilities, in the event of a power disruption, an emergency power system should automatically operate key lights, heat/smoke alarm and duress alarms, the public address system and other essential operating equipment in the facility. Status monitoring of the emergency generator should be provided (“problem” and “running” annunciation) in the building central control. In addition to the facility emergency power system, uninterruptible power supply (UPS) and standby batteries should be provided for the security system. The design should ensure that the security system is capable of a minimum of four hours on emergency electrical power (or as specified by the sheriff).

The Critical Role Played By Security Personnel

The most intelligent architectural design and the most sophisticated security equipment cannot do the job by themselves, however. Ultimately, “people are the main factor in any security program. Equipment, procedures, and architectural security measures are meaningless without capable and trained staff to use them.”⁶

No one involved in security planning should forget that “the selection and training of court security personnel may be the most critical single determinant of the success of a court security plan. Capabilities to perform a variety of routine and non-routine duties, such as taking accurate magnetometer readings, dealing tactfully with the public, applying physical force to remove disorderly persons with minimal injury, and maintaining unobtrusive surveillance of trials in progress must be combined in a relatively few individuals who constitute court security staffs.”⁷ ♦

Endnotes

¹ Joint Statement by Chief Justice Warren Burger and U.S. Attorney General William French Smith; March 11, 1982, before the Judicial Conference of the United States.

² Sobel, Walter A., FAIA, Editor, *The American Courthouse*, Chicago, The American Bar Association, 1973.

³ *The Courthouse: Planning and Design Guidelines*, Hardenbergh, Griebel, et. al., (National Center for State Courts, Williamsburg, VA, 2001)

⁴ Crowe, Timothy D. *Crime Prevention Through Environmental Design*, Butterworth-Heinemann, Boston. 1991, p. 30.

⁵ Ibid, p. 34.

⁶ McMahon, James L., Project Director, *Court Security: A Manual of Guidelines and Procedures*. National Sheriffs’ Association, Washington, D.C. April, 1978, p. 56.

⁷ *Report of the Task Force on Disorders and Terrorism*, Washington, D.C. 1976, p. 275.

Additional Court Security Information

"American Society for Testing & Materials—Draft Standard Guide for Determining Design Criteria for the Physical Protection of a Facility," American Society for Testing & Materials, Philadelphia, PA, August 1996.

Carter, Hon. Richard W., *Court Security for Judges, Bailiffs & Other Court Personnel*, Notebook that covers many specific topics related to court security. Available from Judge Carter, P.O. Box 614, Arlington TX 76004.

Court Security, A Manual of Guidelines and Procedures, National Sheriffs' Association, Washington D.C. (April 1978).

Court Security Guide, National Association for Court Management, Williamsburg, VA (1995).

Court Security and the Transport of Prisoners: A National Study, National Sheriffs' Association, Washington D.C. (October 1995).

Crowe, Timothy D. *Crime Prevention Through Environmental Design*. Boston, MA: Butterworth-Heinemann, 1991.

DOD Antiterrorism Minimum Construction Standards for Buildings.

Fennelly, Lawrence J. *Handbook of Loss Prevention and Crime Prevention, 3rd Ed.* Boston, MA: Butterworth-Heinemann, 1996.

Fennelly, Lawrence J., CPP, *Effective Physical Security, 2nd Ed.* Boston, MA: Butterworth-Heinemann, 1997.

Floyd, William R. *Security Surveys: Guidelines for Evaluating*, Crete, IL: Abbott, Langer & Associates, 1995.

Geiger, Hon. Fred A., *Court Security: A Teaching Guide*, 2nd Appellate District, Illinois.

Griebel, Michael A., Phillips, Todd, S., *Architectural Design for Security in Courthouse Facilities, Annals of the American Academy of Political and Social Science*, Sage Publications, Thousand Oaks, CA. (2001).

Hardenbergh, Don, Griebel, Michael, Tobin, Robert, and Yeh, Chang-Ming, *The Courthouse, A Planning and Design Guide for Court Facilities (2nd Ed.)*, National Center for State Courts (2001).

Mail Room Safety information available through the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention at <http://www.bt.cdc.gov/>

Murphy, Timothy R., Loveland, Geneva Kay, Munsteman, G. Thomas, *Managing Notorious Cases*, National Center for State Courts (1992).

Personal Security Handbook—How You and Your Family Can Minimize Risks to Personal Safety, U.S. Marshals Service, Washington D.C. (1988).

Petersen, William H., and Smith, Barbara E., Ph.D., *Court Security: Training Guidelines and Curricula*, National Sheriffs' Association (May 1991).

Publications by the National Institute of Law Enforcement and Criminal Justice (NILECJ).

Requirements and Specifications for Special Purpose and Support Space Manual including all volumes and addenda: (USMS-RSSPSSM). U.S. Department of Justice, U.S. Marshals Service. Washington, D.C.: Government Printing Office. (2002).

U.S. Courts Design Guide: (USCDG), 1997.

Vulnerability Assessment of Federal Facilities. U.S. Department of Justice, U.S. Marshals Service. Washington, D.C.: Government Printing Office, (1995).



Courthouse photos courtesy DuPage County, Ill., Sheriff's Office

Implementing an Effective Threat Management Process

By

Frederick S. Calhoun and Stephen W. Weston

Extracted from their book *Defusing the Risk to Judicial Officials:*

The Contemporary Threat Management Process

Defusing the Risk to Judicial Officials: The Contemporary Threat Management Process explains how the judiciary can identify, assess, investigate, and manage risks of violence to judicial officials. In any venue, a successful threat management process consists of ten basic elements, each integral to all the others. They compose the golden rules of contemporary threat management. Following them will allow the judicial threat manager to implement an effective threat management process.

Rule 1. Recognize the Need for a Threat Management Process

Courts resolve disputes. They promise a neutral arena for judging emotionally charged controversies. Disputants bring their quarrels before the bench. Each wants his or her claim sustained, each demands vindication. Most who stand before the bar ultimately accept the rulings of the court, however adverse to their own interests. But some cannot. These few care only for the result that most benefits them. That is their justice. Frequently, it clashes with society's justice. When it does, violence can result. The judiciary can hope for little mercy from these discontents. Angry people who believe themselves victims of injustice seldom act justly.

Why do courts need threat management programs? Because the angry and the outraged necessitate it. These individuals, once denied their own selfish sense of justice, may turn to violence for exoneration, vengeance, even salvation. They direct their anger,

their revenge, and their fears at the officials who personify the judicial process: the judges, prosecutors, clerks, and others working within the system. Nor is it simple coincidence that many of these attacks occur at the courthouse. The building itself symbolizes justice, both that dispensed and that desired. Without a competent threat management process to identify, assess, and manage those of violent intent, the justice system chances missing any opportunity to intervene and defuse the risk.

Why do courts need threat management programs? Because the number of these disgruntled individuals appears to be growing. Reports at the federal level show a steady increase throughout the 1990s in inappropriate communications or contacts (IC&Cs) directed toward federal jurists. The number of IC&Cs reported to the U. S. Marshals Service rose from a couple of hundred a year in the early 1990s to over 700 in 2004. Since 1979, three federal judges were killed. In March 2005, a federal judge's husband and mother were killed because the judge dismissed a civil suit. Prior to 1979, only one federal judge was killed. Clearly, a ground shift occurred that resulted in a significant increase in the risk to federal judicial officials.

No comparable national data have yet been compiled on the risks to state and local judicial officials. The evidence suggests these officials have a far harder time of it than their federal cohorts. During the last 35 years, we have documented through newspaper searches the assassination of eight state or local judges. Another thirteen were physically assaulted. Three local prosecutors were killed, four assaulted. At least five law enforcement officers have been killed at local courthouses, 27 assaulted. At least 42 court participants have been killed at local courthouses; 53 assaulted. In March 2005, a Fulton County, Georgia, jail prisoner delayed his escape long enough to seek out the

judge presiding at his trial. After overpowering a deputy sheriff, he killed the judge and a court reporter in the courtroom, then killed another deputy sheriff outside the courthouse.

A 1999 survey of 1,029 Pennsylvania state judges found that 51.8 percent reported being the target of an IC&C sometime during the previous year. Just over a fourth were physically approached; 1.2 percent were assaulted [Neil Weiner, *et al.*]. More disturbingly, over a third admitted they changed their judicial conduct as a result of the experience. Judges compelled to change their judicial conduct sacrifice justice for security. The risk extends beyond the individual jurists and goes directly to the ability of government – state, local, or federal – to ensure justice to its citizenry. Attacks on the judiciary are assaults on the system of justice and, hence, an assault on one of the most crucial elements of democratic self-government. Justice under siege is more than justice denied. It is justice despaired.

Rule 2. Assign Responsibility to Manage Cases to Trained Threat Managers

We emphasize establishing a threat management process, rather than a threat management unit or program, because we do not want to imply any particular size or composition of resources needed to address threat management concerns in any courthouse. Depending on the size of the court and the potential number of IC&Cs that might be reported and the number of cases that might be opened, the threat management process can be handled by a fully staffed unit of threat managers or as a part-time collateral responsibility for one person. Workload is all. It should be the principal criterion for determining the number of personnel and resources dedicated to the process.

Whatever the size or composition, whoever is assigned threat management responsibilities should be trained and the training should be periodically refreshed. The

National Sheriffs' Association offers threat management training, as does Specialized Training, Inc. The national chapter of the Association of Threat Assessment Professionals (ATAP) holds annual conventions in southern California every August. Local ATAP chapters in various cities host one-day seminars. In addition, there is a growing library of research, articles, and books on contemporary threat management.

Rule 3. Provide Training and Liaison with Protectees and Court Staff

The next step in establishing an effective threat management process is to train the court staff in what and how to report IC&Cs. Training the staff helps the threat manager get the initial facts, unembellished by exaggeration or worry, as quickly as possible. The key staff members do not correspond to the usual court hierarchy. Although judges, prosecutors, and chief clerks should be well trained, the majority of reports the threat manager will receive will come from receptionists, mail handlers, perimeter security officers, parking lot attendants, telephone operators, cafeteria staff, and the news stand operator. These are the people who deal most with the public. They are more likely to see or hear or receive any IC&Cs, no matter who is targeted. Training them on what and how to report information will ensure that the threat manager gets reports on IC&Cs timely and accurately.

Rule 4. Create an Incident Tracking System with Well-Documented Files

Controlling the flow of information requires information management. Depending, again, on workload, managing the information can be as simple as an index card system or as sophisticated as a computer database. The system needs to be designed to retrieve information quickly and efficiently. It should include not only demographics on the subject, but also key words or topics used by, or of known interest to, the subject.

The latter may prove crucial in identifying anonymous subjects. At a minimum, the following variables should be captured for each IC&C:

- Case synopsis
- Case specifics
- Method of delivery of the IC&C
- Content and exact quotes from the IC&C
- Suspect demographics
- Target demographics
- Motive, especially in relation to a court case

With information on these variables, the threat manager can manage current cases, cross-reference previous cases, share information on contentious cases or problem individuals as a case works its way up the appellate process or across jurisdictions, and create an institutional memory for that judicial setting. Whatever system is created, it should be designed for easy sharing with other agencies and jurisdictions, ideally as part of regional and national information sharing networks.

Rule 5. Establish Liaison With Other Agencies

It is absolutely vital for the threat manager to reach out beyond the courthouse to make contact with law enforcement agencies, private security firms that provide protective services, and other judicial entities. Keeping lines of communication open with these individuals will provide intelligence information on problem individuals, contentious judicial proceedings, or on those who may pose a risk to the judiciary or its facilities. The threat manager must have information flowing from all sources, both inside and outside the courthouse. Both threat assessments and protective investigations feed on facts; both are voracious eaters. But only through information can the threat manager begin to fill in pieces of the puzzle. Information from disparate sources can link

one IC&C to another and reveal relationships, motives, past behaviors, and previous actions of the subject – in and out of court.

Rule 6. Use Consistent and Valid Threat Assessment Methods

After receiving the initial report of an IC&C and gathering as many facts as are immediately available, the threat manager next must make an initial assessment from which to design the immediate protective response, set a course of fact finding, and begin identifying the most appropriate threat management strategies. A number of experts have developed some facile assessment tools to help the manager think through the case. We have selected four that provide a comprehensive approach when used together. We encourage threat managers to apply each in every assessment. Each allows the threat manager to examine what is known from a different angle. In combination, they provide a thorough assessment of the entire situation. Employing all of these tools helps the threat manager identify what is *not* known, thus giving direction to the protective fact finding.

The four assessment tools address four broad, but related questions. In each case, the threat manager should always ask:

- What are the circumstances and context of the IC&C?
- What are the stakes involved from the subject's point of view?
- Is the subject acting like a Hunter?
- Is the subject acting like a Howler?

Each of these questions focuses on different aspects of the subject's behaviors, motive, and intentions. The first question simply requires the threat manager to describe the IC&C, how it was delivered, to whom it was delivered and directed, what message it says or conveys, and what may have prompted it. The second question deals with what may be at stake in any court case involving the subject. It addresses how desperate or driven toward violence the subject feels. The third question seeks to determine if the subject has

engaged in attack-related behaviors or behaviors common to assassins. The fourth question takes the direct opposite tack. It asks if the subject's behaviors compare similarly to the way non-attackers behave.

Rule 7. Conduct Thorough Fact Finding

Protective fact finding focuses on collecting facts concerning the circumstances of the IC&C and what prompted it, the subject, the target's relation to the subject, the subject's past behaviors, and the subject's current behaviors. The purpose is to gather enough information and evidence to support an accurate and complete re-assessment of the potential risks and the best way to defuse them. The judicial setting contains two valuable aspects, each of which offers a distinct advantage to the threat manager not enjoyed in cases involving other types of public figures.

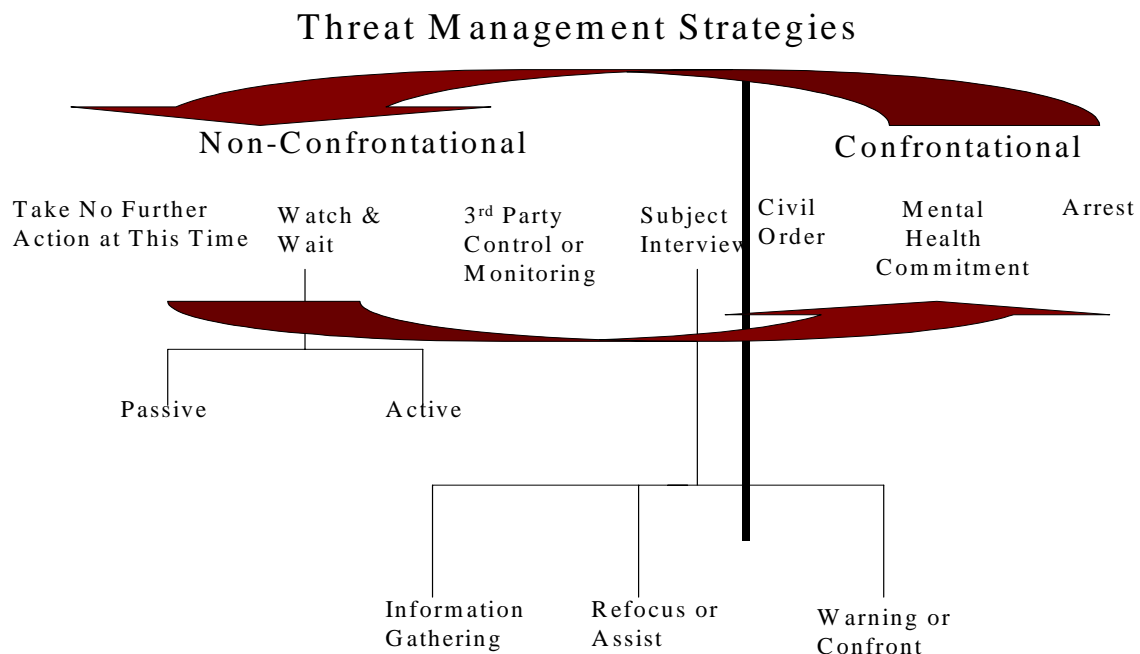
First, the target and his or her staff can be an invaluable source of information about the subject, the subject's issues and motive, and the subject's demeanor under stress. Since most IC&Cs to judicial officials are spawned by a court case, the target often has some knowledge or suspicion about the subject. He or she knows the details of the case. Often, court employees have observed how the subject behaved in court. In addition, court records are readily available in the clerk's office. Reviewing the records in the case may educate the threat manager about the issues and motive prompting the subject to act inappropriately, perhaps even dangerously.

Second, the threat manager should remember that, from the subject's point of view, the courts may be threatening him or her. The IC&C might be a defensive reaction prompted by some action or potential action by the court. The judiciary has the authority to take an individual's freedom, home, and assets. It can order an individual to stay away

from former spouses, offspring, or other family members. It can punish expressions of contempt. People driven to desperation often act desperately. Information for assessing how desperate the subject may feel is readily available from the case files, the target, the IC&C, court staff who have dealt with the subject, the subject's friends and family, and through interviews with the subject.

Rule 8. Apply Threat Management Strategies Flexibly and Intelligently

The strategies for defusing the risk to judicial officials are best conceptualized as different options arrayed along a spectrum. Where each option falls within that range is determined by the option's effect on the subject. The spectrum reaches from discreet and passive defensive measures at one end to intrusive, confrontational acts at the opposite end. They run the gamut from doing nothing that directly affects the subject to using the authority of the law to restrain the suspect. The figure below illustrates the range of threat management strategies available for defusing the risk to judicial officials.



The threat manager should consider all of the strategies, weighing the effectiveness of each given the particular and unique aspects of the case at hand. Each one has specific advantages and disadvantages, and each should be used only when certain conditions apply. We can merely describe each strategy, illustrate it with realistic examples, and give its pros and cons. The threat manager must determine which one offers the best chance for defusing the risk in the case at hand at that particular moment. Once a strategy is played, the threat manager should immediately recognize that the situation has changed *precisely because a strategy has been employed*. The change requires re-evaluating the case, the assessment, and the strategy. This may result in using other strategies. That process is not endless, but often enough it seems like it is.

Rule 9. Communicate with Protectees Professionally, Confidently, and Competently

The threat manager should take care, by word and deed, to reassure the target and his or her staff that the threat manager is a professional problem-solver and that the responses to the incidents are under control. In implementing the appropriate protective responses, the threat manager should never increase the protectee's and the protectee's staff's fears by projecting the wrong attitude or sharing information that they might misinterpret. Frequent updates and open lines of communication with the protectees and their staff will help the threat manager keep them calm, attentive to instructions, and willing to follow the threat manager's lead. Judges especially are used to being in charge and are frequently tempted simply to take charge. Obviously, this should be avoided.

The threat manager should always provide some protective response every time an IC&C is reported. This does not mean putting a protective detail around a judicial official every time his or her phone rings. Protective responses range from providing a

security briefing at a minimum to a full-fledged protective detail or target relocation at the maximum. The selection of the appropriate protective response should be directly proportioned to the assessment and to the findings of any protective investigation.

Always providing some level of protective response serves two purposes. First, it enhances the protectee's security. Even a security briefing helps remind the protectee to take simple precautions and to be aware – and immediately report – any suspicious incidents. Obviously, going up the scale of protective responses adds even more security. Provided each response is in proportion to the threat assessment, the findings of the protective fact finding, and the success of the threat management strategies, then the threat manager will maintain a balance between needed security and limited resources.

Second, always implementing some degree of protective response sends a positive signal to the protectee. It helps underscore the threat manager's professionalism, competence, and concern. That signal will help allay the protectee's fears and give him or her the reassurance that everything necessary is being done.

Rule 10. Manage Cases Appropriately

Threat management cases are seldom open and shut. They begin when an IC&C, not necessarily a crime, has been directed toward a protectee. But they have no climactic point of closing as criminal cases do. Even the most blatant and direct threatener can be arrested and convicted of that crime, but continue threatening or, worse, plotting, from jail. An anonymous subject may direct an IC&C toward a judicial official, then never be heard from again. When can either case be closed? Neither arrest and conviction nor time's cooling effects seem enough to support case closure.

Threat management cases are not about investigating or solving crimes, they are about managing the behavior of an individual. Threat managers do not have a caseload of crimes assigned to them. Rather, threat managers are assigned problem individuals. Consequently, a threat manager's caseload is a hybrid between a criminal caseload and a parole or probation officer's caseload.

Hence, we shy from such traditional terminology as opening or closing a threat management case. Rather, we prefer designating cases as:

- *active*,
- *inactive*,
- *chronic* or *habitual*, or
- *long-term*.

These designations are best suited for managing threat management cases.

Contemporary threat management for judicial officials seeks to avert violence altogether. The judiciary must expand its security from simply fortifying courthouses and reacting to violent attacks. It needs to incorporate an effective threat management process for defusing the risks of violence before the violence erupts. We are not talking about *predicting* violence. Predictions are the province of angels and fools. We advocate establishing procedures to enable the threat manager to identify potential problem individuals, assess the seriousness of the risk, investigate the circumstances, and then devise the appropriate strategies for managing the subject. Implementing an effective threat management process requires the judiciary to follow the 10 golden rules. Doing so will further enhance the judiciary's security.

About the Authors of Defusing the Risk to Judicial Officials:

Frederick S. Calhoun was the lead researcher and principal architect in developing the threat assessment process used by the U. S. Marshals Service for analyzing risks to federal judicial officials. He also developed the Service's policies and procedures for

conducting protective investigations. At the request of the National Sheriffs' Association, Mr. Calhoun coordinated the curriculum and led a nationwide training program on contemporary threat management for local law enforcement. He also wrote the curriculum and led the training of Deputy U.S. Marshal Threat Investigators and their supervisors. Mr. Calhoun earned his Ph.D. from the University of Chicago and is the author of ten books, including *Hunters and Howlers: Threats and Violence Against Federal Judicial Officials in the United States, 1789-1993* and (with Stephen W. Weston) *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent* (available from Specialized Training, San Diego, CA). He can be reached via e-mail at fcalhoun@starpower.net.

Stephen W. Weston is a 31-year veteran of California law enforcement. Since 1991, he has been the supervisor of a specialized unit responsible for the investigation of threats against California state officials. Under his supervision, hundreds of threatening situations are managed every year using the most sophisticated threat management methods. He was an instructor in the contemporary threat management training sponsored by the National Sheriffs' Association. Mr. Weston is currently on the faculty of California State University, Sacramento, in the Criminal Justice Division. In 1996, he graduated from Lincoln Law School in Sacramento and was admitted to the California State Bar. Mr. Weston is the co-author (with Frederick S. Calhoun) of *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent* (available from Specialized Training, San Diego, CA).



Ten Essential Elements for Courtroom Safety and Security

1

Operational Security:
Standard Operating Procedures

2

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

3

Emergency Preparedness and Response:
Continuity of Operations

4

Disaster Recovery:
Essential Elements of a Plan

5

Threat Assessment

6

Incident Reporting

7

Funding

8

Security Equipment and Costs

9

Resources and Partnerships

10

New Courthouse Design



U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Protective Intelligence & Threat Assessment Investigations

*A Guide for State
and Local Law
Enforcement
Officials*

RESEARCH
REPORT



U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Janet Reno
Attorney General
U.S. Department of Justice

Raymond C. Fisher
Associate Attorney General

Laurie Robinson
Assistant Attorney General

Noël Brennan
Deputy Assistant Attorney General

Jeremy Travis
Director, National Institute of Justice

Department of Justice Response Center
800-421-6770

Office of Justice Programs
World Wide Web Site
<http://www.ojp.usdoj.gov>

National Institute of Justice
World Wide Web Site
<http://www.ojp.usdoj.gov/nij>

**Protective Intelligence and
Threat Assessment Investigations:
A Guide for State and
Local Law Enforcement Officials**

★ ★ ★ ★

by Robert A. Fein and Bryan Vossekuil

July 1998



Jeremy Travis
Director

Richard Rau
Program Monitor

Robert A. Fein, Ph.D., is a Psychologist for the U.S. Secret Service, U.S. Department of the Treasury. Bryan Vossekuil is Deputy Special Agent in Charge, Intelligence Division, U.S. Secret Service. This project was supported by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, under award number 92-IJ-CX-0013, and by the U.S. Secret Service, U.S. Department of the Treasury.

The findings, conclusions, and opinions expressed in this document are those of the authors and do not necessarily reflect the official position or policies of the U.S. Department of Justice or the U.S. Department of the Treasury.

NCJ 170612

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Message From the Director, U.S. Secret Service

The U.S. Secret Service is committed to providing a safe environment for each public official it is entrusted to protect. To accomplish this mission, it has developed comprehensive protective programs. The U.S. Secret Service believes that threat assessment and protective intelligence are important aspects of these protection efforts. The purpose of U.S. Secret Service threat assessment and protective intelligence activities is to identify, assess, and manage persons who might pose a threat to those we protect, while the goal of these activities is to prevent assassination attempts.

In carrying out its protective responsibilities, including threat assessment, the U.S. Secret Service works closely with State and local law enforcement agencies. The cooperation, information, and assistance provided through this relationship play a major role in assisting the U.S. Secret Service in fulfilling its responsibilities. At the same time, the U.S. Secret Service has searched for opportunities to further partnerships with State and local police agencies and increase knowledge across all levels of law enforcement.

During the past several years, with the support of the National Institute of Justice and the cooperation of the Federal Bureau of Prisons, the U.S. Secret Service conducted an operational study of the thinking and behavior of the 83 persons known to have attacked or come close to attacking prominent public officials and figures in the United States during the past 50 years. This study, the Exceptional Case Study Project, was recently completed; its findings are leading the U.S. Secret Service to refine and improve its approaches to preventing assassination attempts.

One major product of the Exceptional Case Study Project is this guide, which represents the U.S. Secret Service's efforts to share what it has learned about protective intelligence and threat assessment with State and local law enforcement officials who have

responsibilities in the areas of physical protection or protective intelligence.

The U.S. Secret Service is pleased to join the National Institute of Justice in providing this information to our colleagues in the law enforcement and criminal justice communities. We believe that the ideas and information in the guide may assist persons and organizations responsible for preventing attacks on public officials and figures. We also hope that this information will be useful to other individuals and agencies working to prevent other forms of targeted violence, such as stalking, domestic violence, and workplace violence.

Lewis C. Merletti

Director

U.S. Secret Service

U.S. Department of the Treasury

Message From the Director, National Institute of Justice

Throughout our country's history, persons in the public spotlight have faced danger from others. Elected leaders, political figures, educators, musicians, authors—all have been threatened with attacks on their safety and, in some cases, their lives. In the past, often the only courses of action for threatened individuals were to hire private security, to use publicly provided protection (such as the U.S. Secret Service), and simply to be more aware of the dangers facing them.

In recent years, however, efforts have focused on more proactive prevention techniques—developing ways to identify and neutralize people who pose a threat to public officials and figures. The U.S. Secret Service, in its role as protector of the President and other U.S. and international officials, has pioneered these efforts. The U.S. Secret Service developed the field of threat assessment—the process of investigating and analyzing persons and groups who are interested in and capable of attacking public persons—not only to help it fulfill its mission but also to assist other Federal agencies and State and local law enforcement organizations.

Between 1992 and 1997, the U.S. Secret Service, assisted by the Federal Bureau of Prisons, participated in a collaborative project with the National Institute of Justice, studying assassins and would-be assassins of the past 50 years. The purpose of the Exceptional Case Study Project was to examine in detail the lives of assassins and would-be assassins to determine any common traits. Researchers felt that similarities of characteristics, thoughts, or behaviors among past assassins could be key in helping law enforcement officials better identify which persons could pose a present threat to public figures.

This guide is a product of these efforts; project researchers used the data gleaned from the Exceptional Case Study Project to devise a standard set of protocols and procedures for law enforcement and security agencies responsible for protecting public

persons and others vulnerable to targeted violence. The guide takes agencies through the entire threat assessment process, from designing a protective intelligence program to investigating suspicious persons to closing a case. The National Institute of Justice and the U.S. Secret Service hope that State and local law enforcement organizations and other criminal justice practitioners will find this guide useful as they work to prevent and deter those who would engage in violence such as stalking, workplace violence, or domestic violence.

Jeremy Travis

Director

National Institute of Justice

U.S. Department of Justice

Acknowledgments

The authors wish to acknowledge the support of the National Institute of Justice, especially the guidance of Richard Rau, Ph.D., and the editorial support of the NIJ publications unit.

Staff from the Federal Bureau of Prisons assisted in obtaining records and interviewing study subjects. The authors especially thank Daniel Cowell, M.D.; Ruth Westrick-Connolly, M.D.; Sally Johnson, M.D.; Casey Skvorc; and staff at the Federal Medical Centers in Rochester, Minnesota, and Butner, North Carolina.

Many persons within the U.S. Secret Service supported the authors' efforts and contributed to the success of the Exceptional Case Study Project (ECSP). The authors especially thank Director Lewis C. Merletti; former Directors John R. Simpson and Eljay Bowron; Assistant Directors H. Terrence Samway, Michael Smelser, David Lee, and Stephen Sergek; Special Agents in Charge Jane Vezeris and Dale Wilson; Deputy Special Agent in Charge James Lucey; Special Agents Marty Allen, Steve Amico, Al Baker, John Berglund, Mike Garduno, Paul Gebicke, and George Sexton; Intelligence Research Specialist Chris Wallace; Research Section Chief Margaret Coggins, Ph.D.; Researchers Angela Macdonald and Joseph Gerston; Senior Intelligence Research Specialist Lynn Zimney; Archivist Michael Sampson; Supervisory Visual Specialist Ed Ross; and Visual Information Specialists Jeff Clemente, Bob Fulk, MacKenzie Kearney, and Patrick Nolan. A special note of thanks is due Assistant Director Sergek, who reviewed ECSP drafts and provided numerous comments.

Pamela Clark Robbins and Henry Steadman, Ph.D., of Policy Research Associates, Inc., provided incisive suggestions and key support at each stage of this project.

Shervert Frazier, M.D., provided invaluable information on violence that shaped the authors' understanding of assassination behaviors.

Gavin de Becker shared information and insights and made many helpful comments about an early draft of the guide.

The authors also wish to thank several other people who reviewed early drafts of the guide, including Randy Borum, Psy.D., Frederick Calhoun, Ph.D., Michael Gelles, Psy.D., Chris Hatcher, Ph.D., Robert Kasdon, Paul Kelly, David Noznesky, Lieutenant Tom Taylor, and Patrick Wolfe. Their comments strengthened the guide.

The authors are grateful to Rita Premo of Aspen Systems Corporation for her editorial assistance.

Finally, the authors wish to acknowledge the contribution of Gwen Holden, who provided both enormous support and great expertise. Her vigorous and skillful editing helped shape the guide into a useful document for Federal, State, and local law enforcement and security professionals.

Contents

Message From the Director, U.S. Secret Service iii

Message From the Director, National Institute of Justice v

Acknowledgments vii

Chapter 1. Introduction 1

 The Problem 3

 Exceptional Case Study Project 4

 Threat Assessment Protocols 6

Chapter 2. Assassins and Assassination Behavior 9

 The Assassin 11

 Myth 1 12

 Myth 2 13

 Myth 3 14

 Key Observations on Assassins 15

 Attacks are the product of organized thinking
 and behavior 16

 Attacks are the means to a goal 16

 Motive and target selection are directly connected 19

 Who is dangerous? 20

Chapter 3. Elements of a Threat Assessment Program 21

 Effective Design 23

 Key Functions of a Protective Intelligence Program 25

 Identification 25

 Assessment 27

 Case management 28

 Functions and Approaches of the Case Investigator 29

Investigative skill	29
Corroboration.....	30
Common sense	30
Building a Database and Sharing Information	31
Chapter 4. Conducting a Threat Assessment	
Investigation	33
Opening a Case	35
Inappropriate or unusual interest	35
Threats	36
Investigating a Case	37
Interviewing the subject	37
Content of a protective intelligence investigation.....	39
Chapter 5. Evaluating a Threat Assessment Case	47
Principles to Guide a Protective Intelligence Evaluation	49
Questions to Ask in a Threat Assessment	50
Protection	52
Chapter 6. Managing a Protective Intelligence Case	53
Monitoring, Controlling, and Redirecting the Subject	55
Ending Monitoring	57
Sources of postassessment information	57
Closing a Case	58
Conclusion	58



CHAPTER *1*

Introduction



Threat assessment is a developing field pioneered by the U.S. Department of the Treasury's U.S. Secret Service, which is charged with protecting the President of the United States and other U.S. and foreign leaders. Threat assessment measures involve investigation and analysis of situations and individuals that may pose threats to persons in public life. In 1992, the Secret Service, in partnership with the National Institute of Justice and with assistance from the Federal Bureau of Prisons, began the Exceptional Case Study Project (ECSP), a 5-year study to examine the thinking and behavior of individuals who have attacked or approached to attack prominent public officials or figures in the United States since 1949.¹ ECSP findings reveal general threat assessment information relating to attacks on public officials and figures, while suggesting that broader application of threat assessment protocols by Federal, State, and local law enforcement officials could help anticipate and prevent other crimes, such as stalking and workplace violence.

Drawing from project findings, this guide describes an approach to threat assessment and the protective intelligence investigative process that can be of assistance to Federal, State, and local law enforcement and security professionals with protective intelligence responsibilities. Though not intended to serve as an operations manual, the guide presents information and ideas about developing and implementing protective intelligence programs and activities. Information about the thinking and behavior of persons who have attacked or come close to attacking public officials and figures can help refine law enforcement operations related to preventing and investigating violence and threats of violence.

The Problem

Assassination of political leaders and other public figures has been a significant problem in the United States. Since 1835, 11 attacks on U.S. presidents (4 of them resulting in the death of the President) have occurred. Since 1949, two attacks on Presidential candidates have been attempted, in addition to two attacks on Members of Congress, several assassinations of national political

leaders, a number of attacks on State and local elected officials, several murders of Federal and State judges, and several well-publicized attacks on celebrities and business leaders. These attacks do not include many other individuals who presented themselves as warranting serious concern. Each year, Federal, State, and local law enforcement officials and private security officers intercede with thousands of individuals who demonstrate inappropriate or unusual interest in a public official or figure. Some of these individuals were intercepted within lethal range of a target just before they attempted to mount an attack.

Although substantial academic literature on assassination exists, little has been written about the thinking and behavior of assailants who attempt attacks on prominent persons. For example, how do attackers select their targets? What are their motives? How do they plan their attacks? How do these persons assess the security barriers that face them? What communications, if any, do they make before their attacks? To what extent do symptoms of mental illness affect their actions?

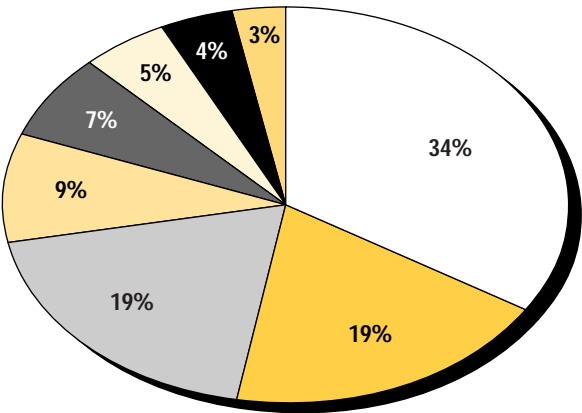
Planned, targeted attacks are not confined to those involving prominent public officials and celebrities. Tragically, such attacks are a frequent feature of interpersonal violence in this country today. Cases involving stalking, domestic violence, workplace violence, and bias-motivated criminal activity involve planned—often violent—attacks on intentionally selected targets.

Exceptional Case Study Project

The study examined the thinking and behavior of all 83 persons known to have attacked or approached to attack a prominent public official or figure in the United States from 1949 to 1996. During this time period, 74 attacks and near-lethal approaches occurred.² Six attacks were carried out by 16 individuals who were members of groups. Sixty-eight of the attacks and near-lethal approaches were carried out by 67 individuals acting alone. (One individual attacked two public figures.) Targets of these individuals included Presidents, other officials protected by the Secret Service, Members of Congress, Federal judges, prominent national political

leaders, State and city officials, business executives, and entertainment, sports, and media celebrities. (See exhibit 1.) All targets were selected because they were prominent persons.

Exhibit 1. Targets of Modern American Assassins, Attackers, and Near-Lethal Approachers, 1949–96



Target	Number*	Percent
<div></div> President	25	34
<div></div> Movie, sports, and media celebrities	14	19
<div></div> Secret Service protectees other than the President	14	19
<div></div> Other national political figures	7	9
<div></div> Members of Congress	5	7
<div></div> Federal judges	4	5
<div></div> Business executives	3	4
<div></div> State and city officials	2	3

All available criminal justice, court, social services, mental health, and public records were gathered and analyzed for each individual studied. Additionally, 24 of the 83 individuals were interviewed.

*Note: Total number was 74.

ECSP information gathering and analysis focused on seven major questions:

- How did these individuals develop the idea of assassination, and how did they move from the idea of assassination to lethal or near-lethal action?
- What were the individuals' motives?
- How did the individuals select their targets?
- How did the individuals plan their attacks?
- What communications, if any, did individuals make before their attacks or near-lethal approaches?
- What role, if any, did symptoms of mental illness play in individuals' assassination behaviors?
- Were there key life experiences or incidents that appeared to affect individuals' assassination interests or behaviors?

ECSP findings could be used to help law enforcement and security professionals throughout the United States reevaluate their methods of investigating assassinations and kidnappings, formulating protective strategies, and gathering protective intelligence. This guide describes the following:

- Important information about assassins and assassination behaviors.
- Elements of an effective protective intelligence system.
- Specialized threat assessment investigations.

Threat Assessment Protocols

Law enforcement organizations, private security experts, and the potential targets of violent attacks spend considerable resources on personal protection measures such as enhancements in physical security; 24-hour-a-day physical protection for themselves, their home, and their office; and/or periodic protection. They also may include specialized personal safety training for potential targets.

Threat assessment or protective intelligence is the process of gathering and assessing information about persons who may have the interest, motive, intention, and capability of mounting attacks against public officials and figures. Gauging the potential threat to and vulnerability of a targeted individual is key to preventing violence. Among criminal justice functions, threat assessment holds great promise for determining vulnerability and guiding interventions in potentially lethal situations.

The primary goal of every protective intelligence investigation is to prevent an attack on a potential target. By using a combination of investigative skill, corroboration, and common sense, a protective intelligence investigator can gather the information and evidence to make a thoughtful assessment of the threat an individual may pose to a target. Once an assessment is made, a plan can be developed and implemented to monitor the individual and to intervene, as appropriate, to prevent an attack. Attention to the individual's motives and attack-related behaviors and to the systems (family, work, community, criminal justice, mental health, and social services) that the individual is involved with are key to assessing and managing a potential threat.

Building and maintaining the organizational capacity to conduct protective intelligence investigations at the Federal, State, and local levels takes careful conceptualization, planning, and oversight by experienced law enforcement and security agency managers. Once developed, a protective intelligence program will serve as a key component of a comprehensive protection program to prevent targeted violence.



CHAPTER 2

Assassins and Assassination Behavior



Three days after a Presidential candidate visited a small Southern city in September 1988, an anonymous letter writer ordered the candidate to drop out of the Presidential race. The letter stated that the writer had attended the candidate's rally with a gun and had stood within shooting range of the candidate. "I didn't shoot this time," said the letter. "I will the next." Enclosed with the letter were three photographs of the rally. Investigative analysis suggested that the photographer was standing within 100 feet of the candidate.

A receptionist in the Governor's office reported that a well-dressed man came to the office, gave his name, and demanded a meeting with the Governor. Asked why he wanted to see the Governor, the man stated, "If he won't meet with me by next Thursday, I will place him under arrest." The man then left the office.

A man called the police to report that a female tenant in his apartment building appeared to be "fixated" on a popular film actor. He said that when he was asked to fix a broken toilet in her apartment about a month ago, he noticed that the walls were covered with posters of the actor. The day before, another tenant had told him that the woman said that "X [the actor] and I will both be dead in a week." When the man read in the newspaper that X was scheduled to make an appearance at a benefit dinner in the city early the following week, he decided to contact the police.

These are examples of situations that come to the attention of Federal, State, and local law enforcement authorities and security managers. Any of these cases may present a risk to a target. The overwhelming majority of cases that come to law enforcement's attention do not result in attacks. But, a few cases do culminate in assassination attempts. Sometimes, individuals and groups attempt assassinations without becoming known to authorities before they attack.

The Assassin

Three prevalent beliefs about assassination exist in popular culture, largely unsupported by data that have been gathered and

analyzed about attackers of public officials and figures in the United States. Critical thinking about assassination behaviors proves these beliefs to be myths.

Myth 1: There is a profile of “the assassin.”

Fact: Attackers and near-lethal approachers do not fit any one descriptive or demographic profile (or even several descriptive or demographic profiles).

Much has been written about profiles of assassins, but in reality there are no accurate descriptive or demographic profiles of American assassins, attackers, and near-lethal approachers. American assassins and attackers have been both men and women of various ages, educational backgrounds, employment histories, and other demographic and background characteristics.

ECSP findings about the histories and personal characteristics of attackers and near-lethal approachers include the following:

- Their ages ranged between 16 and 73.
- Almost half had attended college or graduate school.
- They often had histories of mobility and transience.
- About two-thirds were described as socially isolated.
- Few had histories of arrests for violent crimes or for crimes that involved weapons.
- Few had been incarcerated in Federal or State prisons before their attack or attempt to attack a public figure.
- Most had histories of weapons use, but few had formal weapons training.
- Many had histories of harassing other persons.
- Most had histories of explosive, angry behavior, but only half of the individuals had histories of physically violent behavior.
- Many had indicated their interest in attacking a public figure to someone else.

- They often had interests in militant or radical ideas and groups, though few had been members of such groups.
- Many had histories of serious depression or despair.
- Many were known to have attempted suicide or to have considered suicide at some point before their attack or near-lethal approach.
- Almost all had histories of grievances and resentments, many directed against a public official or figure.

Although there is no such thing as an assassin profile, potential attackers often engage in many of the same behaviors and actions before their attacks. Mounting an attack on a prominent person requires a number of preparatory decisions and activities—attack-related behaviors. For instance, a potential assassin must choose a target, learn where the target is going to be, choose and secure a weapon, survey security, develop an attack plan, and consider whether and/or how to escape. Although not every ECSP attacker and near-attacker engaged in all of these activities and behaviors, most engaged in several of them.

Myth 2: Assassination is a product of mental illness or derangement.

***Fact:* Mental illness only rarely plays a key role in assassination behaviors.**

Many believe that attacks on public figures are deranged behaviors, without rational or understandable motives; they therefore believe that perpetrators of these crimes must be mentally ill. In most cases, however, mental illness does not appear to be a primary cause of assassination behavior. Attacks on prominent persons are the actions of persons who see assassination as a way to achieve their goals or solve problems, which requires a fairly rational process.

Most near-lethal approachers and the great majority of assassins were not mentally ill—none were models of emotional well-being, but relatively few suffered from serious mental illnesses that caused their attack behaviors.

In almost every case—even those in which the attackers were seriously mentally ill—an attack was a means to achieve an end, such as calling attention to a perceived problem. Moreover, in cases where mental illness clearly played a role in assassination attempts, symptoms of mental illness generally did not prevent the person from engaging in attack-related activities, such as rationally developing an attack strategy. In most situations involving persons with severe and untreated mental illness, the symptoms disable the person's usual problem-solving abilities. However, among mentally ill ECSP attackers and near-lethal approachers, most remained organized and capable of planning and mounting an attack.

Mental health histories of ECSP attackers and near-lethal approachers include the following:

- Many had contact with mental health professionals or care systems at some point in their lives, but few indicated to mental health staff that they were considering an attack on a public official or figure.
- Almost half had histories of delusional ideas, but few of these ideas led directly to a near-lethal approach or attack.
- Few had histories of command hallucinations (imagined voices ordering the individual to take action).
- Relatively few had histories of substance abuse, including alcohol abuse.

Myth 3: The persons most likely to carry out attacks are those who make direct threats.

Fact: Persons who *pose* an actual threat often do not *make* threats, especially direct threats.

People who study assassination often associate threateners with attackers, as if the two are the same. Many assume that those who *make* threats *pose* real threats. Although some threateners may pose a real threat, usually they do not. However, most importantly, those who *pose* threats frequently *do not make* threats.

- None of the 43 assassins and attackers communicated a direct threat to the target before their attack.
- Fewer than one-tenth of all 83 attackers and near-lethal approachers communicated a direct threat to the target or to a law enforcement agency.
- Two-thirds of the assassins and near-lethal approachers were known to have spoken or written in a manner suggesting that they were considering an attack. Would-be assassins told family members, friends, colleagues, and associates about their thoughts and plans, or they wrote down their ideas in journals or diaries.

These data do not suggest that investigators should ignore threats that are communicated to or about public officials or figures. Many persons may have been prevented or deterred from taking action because of a prompt response to their threatening communications. However, careful attention should also be paid to identifying, investigating, and assessing anyone whose behaviors suggest that he or she might pose threats of violence, even if the individual does not communicate direct threats to a target or to the authorities.

Key Observations on Assassins

Three key observations about assassins and their behaviors emerged from the ECSP study:

- Assassinations and attacks on public officials and figures are the products of understandable and often discernible processes of thinking and behavior.
- Most people who attack others perceive the attack as the means to a goal or a way to solve a problem.
- An individual's motives and selection of a target are directly connected.

Attacks are the product of organized thinking and behavior

Almost without exception, assassinations, attacks, and near-attacks are neither impulsive nor spontaneous acts. The notion of attacking the President does not leap fully formed into the mind of a person standing at a political rally attended by the President. Ideas of assassination develop over weeks, months, even years, and are stimulated by television and newspaper images, movies, and books. Potential assassins seek out historical information about assassination, the lives of attackers, and the protectors of their targets. They may deliberate about which target—and sometimes targets—to choose. They also may transfer their interest from one target to another.

After selecting a target, attackers and near-lethal approachers develop plans and sometimes rehearse before mounting an attack. Often, their days are shaped by their planning activities: What kind of weapon shall I use? Where will the target be? How will I get close? What should I wear? What should I carry with me? Should I leave a letter in case I am killed? For some would-be attackers, such thinking dominates their lives, providing a sense of meaning or a goal that will end their emotional pain.

Frequently, thinking about assassination is compartmentalized; some potential assassins engage in ongoing internal discussions about attacks while maintaining outward appearances of normality. In every ECSP case, assassination was the result of an understandable and often identifiable process involving the attacker's pattern of thoughts, decisions, behaviors, and actions that preceded the attack.

Attacks are the means to a goal

Most people who attack others consider violence the means to a goal or a way to solve a problem. The problem may be that the potential perpetrator feels unbearably unhappy, enraged, overwhelmed, or bereft. If the person views violence as an acceptable or permissible solution, the risk of violent action increases.

Violence—especially assassination—is an event in which a *person*, triggered by an *event* or change, and operating in a *situation* that facilitates, permits, or does not prevent violence, takes action against a designated *target*. These four elements—the potential attacker, event, situation, and target—form the basis for a threat assessment investigation.

The potential attacker. Determining the risk of targeted violence, such as assassinations, begins with gathering information about the potential attacker. In threat investigations and assessments, a key concern is how the person has dealt with *unbearable* stress in the past.

People have many options for dealing with stress: resting, working, exercising, sleeping, changing activities, seeking family support, making contact with friends, etc. However, what happens when the usual means of dealing with stress are not available, do not work, or are not pursued and a person considers life unbearably stressful? At such a time, four reactions are possible. A person might become:

- Physically ill.
- Psychotic or otherwise out of touch with reality.
- Suicidal or self-destructive.
- Violent to others or homicidal.

The event. Investigators should also examine past traumatic events in the life of the individual, particularly those that caused life to seem unbearably stressful. These might include major changes such as:

- Losses of significant relationships (the end of an intimate relationship, death of a parent, or loss of a child).
- Changes in financial status (the loss of a job or threatened financial disaster).
- Changes in living arrangements (being released from an institution, for example).
- Feeling humiliated or being rejected, especially in public.

Major adverse changes in life circumstances, such as losses, failures (real or perceived), and rejections appear to stimulate attack-related behavior—more than half of the ECSP subjects were known to have experienced a major life stressor event in the year before their attack or near-lethal approach.

People deal with life changes and events differently. What might cause one person major worry and distress is met with acceptance by another. To determine whether an individual may be a cause for concern, three questions must be answered: What events or changes led the individual to perceive life as unbearably stressful? How did he or she respond to these events? What is the likelihood that such events or changes will recur in the individual's life?

The situation. The third factor to consider is the individual's specific situation at the time of peak stress. Do people around the person support, permit, or ignore the threat of violence? Do family, friends, colleagues, or supervisors say—directly or indirectly—that violence is not a solution to problems and is not permitted? Or is the possibility of violence condoned, accepted, or ignored? People around a person who is acutely at risk of behaving in a violent manner can act to prevent violence.

The target. When conducting a threat assessment, protectors and investigators must also pay attention to the individual's choice of a potential target, assuming the individual has selected a target. The following questions should be addressed:

- How well is the target known to the individual? Is the individual acquainted with the target's work and lifestyle patterns? Is that information readily available, as in the case of many public officials or highly visible public figures?
- How vulnerable is the target to an attack? What changes in the target's lifestyle or living arrangements could make attack by the individual more difficult or less likely?
- How sophisticated is the target about the need for caution? How concerned about safety is the target? How concerned are those around the target (such as family or staff)? How

responsive is the target likely to be to the advice of law enforcement and security professionals?

Motive and target selection are directly connected

Contrary to the general perception, few assassins in the United States—even those targeting major political leaders—have had purely political motives. Other than the Puerto Rican nationalists who attacked President Harry S. Truman in 1950 and Members of Congress in 1954, most recent assassins, attackers, and near-lethal approachers held motives unrelated to politics or political causes. ECSP's examination of the thinking and behavior of the 83 American attackers and near-lethal approachers identified 8 major motives, most of which are personal:

- To achieve notoriety or fame.
- To bring attention to a personal or public problem.
- To avenge a perceived wrong; to retaliate for a perceived injury.
- To end personal pain; to be removed from society; to be killed.
- To save the country or the world; to fix a world problem.
- To develop a special relationship with the target.
- To make money.
- To bring about political change.

Many attackers and near-lethal approachers craved attention and notoriety, while others acted to bring attention to a particular problem. A number of assailants of public officials and figures were consumed with seeking revenge for perceived injuries or harm. A few attacked or nearly attacked public officials or figures in hopes of being killed by law enforcement or being removed from society by being incarcerated. Several believed that assassinating their target was a way to save the world. Others responded to beliefs or imagined voices that they felt ordered them to attack a national leader. A number of subjects approached a celebrity with a weapon to try to force the target into a special relationship. Finally, a few attacked public officials or figures for

money, either because they were paid to kill the target or as part of an attempt to secure ransom money.

Targets are selected on the basis of motive, not primarily because of feelings about or hostility toward a particular target or office. Whether an individual likes a particular elected official may be irrelevant if the individual's motive is to achieve notoriety. "I would have voted for him," said one would-be attacker, "if I hadn't been in jail charged with trying to kill him."

Consistent with their motives, many ECSP attackers and would-be attackers considered more than one target before moving to attack. For example, several individuals whose primary motive was notoriety considered attacking public officials like Governors and Members of Congress before ultimately deciding to attack the President or Vice President; they calculated that an attack on the President or Vice President would receive more attention. Assaultants often made final decisions about whom to attack because an opportunity for attack presented itself or because they perceived another target was unapproachable.

Who is dangerous?

Not all "dangerous" persons should be considered dangerous to a particular public official or figure. Clearly, a man who is serving multiple life sentences for killing bank customers during a robbery is a dangerous person, but he may not pose a threat to a Governor or to an entertainer. Therefore, threat investigators need to consider if he has a motive to attempt such an attack. If he does, the next question is: What is his current and foreseeable ability to attack a Governor or entertainer?

Who, then, is dangerous to public officials and figures? Generally, a person who thinks that attacking a public official or figure is a desirable, acceptable, or potentially effective way to achieve a goal can be considered a potential assassin. If such a person has or develops the capacity to mount an attack on a public official or figure, the threat increases. Changes in thinking about the acceptability or effectiveness of attacking, or changes in ability to attack, may decrease the threat posed.



CHAPTER 3

Elements of a Threat Assessment Program



Effective Design

Designing and implementing a protective intelligence program in a law enforcement or security organization involves two steps. The first step is to define the problem, conceptualize the program and its functions, and establish objectives. The next step is to assess what capabilities are needed to implement the program and to plan so that essential functions can continue over time.

In completing the first step, certain questions must be answered:

- How does the organization define its protective responsibilities? What protective responsibilities does the organization now have? What responsibilities is it likely to have?
- What approaches to protection are currently being used? What kinds of protective services and programs are most likely to fulfill the organization's responsibilities?
- What is the legal basis for protection?
- How often is the organization faced with the task of responding to a threat or a concern about possible violence directed against a public official or figure?
- What currently happens when a threat is received by a protected person's office?
- What should occur when an individual who might be interested in harming a public official or figure comes to attention? For instance, who should be notified?
- Is the organization faced with other targeted violence investigative concerns such as stalking or workplace violence?

Protective services encompass a range of functions, including protective intelligence and physical protection, designed to shield potential targets of violent attacks or assassinations. Visible protectors, such as uniformed officers and security agents, are deployed to defend against any attempted attack on a protected person. Other physical protection measures, such as

metal detectors, may keep persons with weapons away from a protected person and deter would-be attackers from trying to approach with a weapon.

Protective intelligence—a less visible aspect of protection—consists of programs and systems aimed at identifying and preventing persons with the means and interest to attack a protected person from getting close enough to mount an attack and, when possible, reducing the likelihood that they would decide to mount an attack. Protective intelligence programs are based on the idea that the risk of violence is minimized if persons with the interest, capacity, and willingness to mount an attack can be identified and rendered harmless before they approach a protected person. This involves three key functions:

- *Identification* of persons who might pose a threat.
- *Assessment* of persons who are identified as a potential threat.
- *Case management* of persons and groups deemed a threat to a protected person.

The second step in developing a threat assessment program involves determining what is needed to complete protective intelligence tasks, examining what is needed to conduct threat assessments, and deciding how to maintain the threat assessment program. Again, several questions must be answered:

- Who will carry out protective intelligence responsibilities? What kind of staffing is needed?
- How will the knowledge and expertise developed by protective intelligence investigators be maintained and shared over time?
- How will new investigators learn, and how will experienced investigators teach?
- What balance of specialized threat assessment expertise and general investigative experience is desirable?
- Can the protective intelligence program build ways to learn from its experiences?
- How will case information be stored and retrieved for individual and aggregated case analysis?

The needs of agencies responsible for protective intelligence mainly depend on their activities. For instance, an organization like the U.S. Secret Service, with responsibility for protecting the President and other national leaders, needs to have the ability to respond immediately to information that a person or group may pose a threat to a protected person. Likewise, a police department in a major city may have a substantial need to fulfill ongoing protective responsibilities as well as intermittent needs to support other targeted violence investigations. A security organization responsible for protecting celebrities may require extensive protective intelligence abilities. Smaller security organizations or those with limited or episodic protective responsibilities may have less extensive needs.

Key Functions of a Protective Intelligence Program

A protective intelligence program involves three key functions: identifying those who might pose a threat, investigating and assessing those individuals, and engaging in case management of those who have been deemed a threat to a protected person.

Identification

Identification is the process by which persons who might present a risk to a public official or figure come to the attention of agencies responsible for protective intelligence.

Some persons self-identify—they call, write, e-mail, or approach a public official or figure or indicate an unusual or inappropriate interest in a person. These individuals often give their names or provide other information that leads to easy identification.

The threatener—someone who communicates a direct, indirect, or conditional threat—is the classic example of a self-identifier. Such a person may threaten for various reasons: to warn of a possible attack, to ask to be stopped, to demand help or attention, to express frustration or anger, or to communicate distress. Threats should always be investigated; even if a threat is not an early

warning of attack, making a threat is usually a violation of law, which is a valid reason for opening an investigation.

Other persons self-identify by expressing an inappropriate interest in a public official or figure. They may feel that they have (or should have) a special relationship with the potential target, a unique assignment or role to play, or extraordinary information or expertise that must be shared directly with the public official or figure.

In addition to self-identifying, people also come to the attention of law enforcement by being noticed by others who:

- Recognize that the behavior of the individual is of concern.
- Believe that the individual should be brought to the attention of authorities.
- Understand that authorities want to know about persons who might pose a risk to public officials or figures.
- Know how to contact the proper law enforcement or security organization (or know someone who knows how to contact authorities).

Individuals can be brought to the attention of the authorities by various second parties, including other law enforcement agencies, State agencies, security professionals, family members, neighbors, coworkers, mental health practitioners, and correctional staff. But before this can happen, protective intelligence program staff must decide on identification criteria—which kind of persons the unit wants to be informed about: Those who make threats against a protected person? Those who indicate to others that they are considering an attack on a protected person? Those who demonstrate inappropriate interest in a protected person?

Once identification criteria are determined, decisions must be made about education: Who should be informed about how to report cases of potential concern? What should family members, associates, and staff of a public official or figure know? What should be said to the public about reporting cases of potential concern?

Liaison between protective intelligence agencies and the public is a key function of the identification process. Law enforcement and security agencies will receive information only if the public is aware that they have protective intelligence capacities and know how to contact protective intelligence personnel.

In addition, liaison is important within a given organization and with other organizations. Access to information is increased when the protective intelligence unit previously has engaged in liaison efforts designed to educate organizations and individuals who may have information on potential threats about the mission and functions of the protective intelligence unit. People and organizations with information may be more willing to share information if they are aware of the responsibilities of the protective intelligence unit and if they previously have met or become acquainted with protective intelligence staff. For instance, information from other city agencies about possible threats to the mayor's safety is more likely to come to the police department if staff know that the police department has a protective intelligence capacity. In a corporate environment, reports about persons of possible concern will come more readily to those responsible for an executive protection unit if employees know that the unit exists and how to contact unit staff.

Assessment

After an individual who poses a possible threat to protected persons comes to the attention of agencies responsible for protective intelligence, an initial evaluation is conducted and a decision is made about whether to conduct an investigation. If an investigation is opened, investigators gather information about the individual and then evaluate the information collected to determine whether the individual poses a threat to a protected person. The quality of an assessment is related to both the relevance and the range of information gathered. Key facts of a case should be authenticated and corroborated, with appropriate investigative skepticism about the credibility, accuracy, and veracity of witnesses and informants.

Sources of information. Protective intelligence investigators should make use of all the information available about an individual that will help them answer the fundamental question of threat assessment investigations: Does this subject pose a threat to protected persons? Investigators should emphasize factual data that can be corroborated, rather than the opinions of those who know (or purport to know) the individual.

Sources of information include interviews with the individual and those who have had contact with or appear to have information about the individual (employers, coworkers, neighbors, relatives, associates, caregivers, arresting police officers), records from agencies and institutions that have had contact with the individual, writings by or about the individual, and receipts from the individual's purchases and travels.

A variety of strategies and tools are used in protective intelligence investigations, including interviews; searches of people, residences, automobiles, etc.; background checks; reviews of weapons purchases, credit card purchases, phone records, and travel verifications; and consultations with threat assessment professionals.

The processes of information gathering and evaluation occur simultaneously; they are distinct, but influence each other. Newly developed information affects the ongoing evaluation of the risks an individual poses to protectees. At the same time, the evaluation process may suggest new investigative leads or directions of inquiry.

Case management

When sufficient information is gathered to permit a full evaluation, a decision is made about whether the individual being investigated poses a threat to a protected person. If investigators believe that the individual does not pose a risk, the investigation ends and the case is closed. However, information about closed cases should generally be retained for a period of at least several years. An individual may come to an agency's attention as a

potential threat again, in which case information from the previous investigation may be invaluable.

If the individual is deemed a threat, a plan to manage the individual and possible risks is developed and implemented. Such a plan may be as simple as periodically confirming the whereabouts, for example, of an individual confined to a correctional or mental health facility for an extended period of time. A case management plan also may involve a pattern of specified contacts with the individual and others around the individual—such as family members, police officers, coworkers, and caregivers—designed to prevent the individual from approaching a protected person and to decrease the risk of violence posed by the individual. In developing and implementing a case management plan, consultation with threat assessment and other professionals is useful. In all cases, the plan should include informing targets or their designated protectors.

Once developed, a case management plan is implemented until the protective intelligence agency decides that an individual no longer poses a threat of violence. At that point the investigation is concluded and the case is closed.

Functions and Approaches of the Case Investigator

Protective intelligence investigations should be based on three principles—investigative skill, corroboration, and common sense—that guide investigators as they develop and execute protective intelligence operations.

Investigative skill

Protective intelligence investigations should be approached with the inquisitiveness and skepticism that are hallmarks of other investigations. The central goal of a protective intelligence investigation is to determine whether an individual has the motive and means to develop or act on an opportunity to attack a protected person. A primary task of the investigator is to gather information, some of which may later be used as evidence, that

can be used to determine whether the individual poses a threat to a protected person.

Corroboration

The second component of protective intelligence work is corroboration. Significant facts of a case, including the statements of an individual who may pose a threat, should be corroborated whenever possible. This means, for example, that a report that the individual traveled to a city on a given date should be viewed skeptically until corroborated; investigators should attempt to secure copies of travel and lodging receipts, statements of credible witnesses who saw the individual, and so on. If the individual is to be interviewed, questions regarding recent activities that would form the basis for corroboration may also help the investigator form a judgment about the accuracy and truthfulness of the information gathered during the interview.

Common sense

Protective intelligence investigations, by their nature, involve considerable discretion and judgment on the part of the investigator. Thus, common sense is necessary. For instance, common sense would indicate that a person who attends three events where a protected person is speaking during a period of several weeks (the last time with a pistol) and who has no plausible explanation for attending these events is a subject for concern—even if no direct threats have been made against the protected person.

Likewise, a man serving multiple life sentences in a maximum-security State prison for murdering three people who writes the Governor saying, “I am committed to killing you by any means necessary,” may have motives for writing other than a desire to kill the Governor. Common sense suggests that the letter writer may be a dangerous person. However, common sense also leads an investigator to explore other possible motives that might have led the prisoner to threaten the Governor, such as the wish to secure transfer to another prison or to increase his status in the prison population. After such an inquiry, an investigator is better

prepared to conclude whether the letter writer poses a threat to the Governor.

Building a Database and Sharing Information

Information about the persons who are subjects of threat assessment investigations should be organized and maintained in a manner that permits search capabilities, efficient retrieval, and analysis. Some individuals come to the attention of the authorities more than once, sometimes months and even years after the initial investigation was completed and the case closed. In these cases, prompt retrieval of case materials fosters an informed decision of what additional investigation, if any, is needed.

Developing a database also permits later analysis of behavior patterns that come to the attention of threat assessment investigators. A database containing both anecdotal and statistical information about individuals who have been investigated could promote future development of training materials and teaching programs for agencies with protective intelligence and physical protection responsibilities.

Creating a database of threat assessment cases is also useful for interagency cooperation. Attackers and would-be attackers often consider multiple targets, who may live in different jurisdictions with various law enforcement agencies and security organizations responsible for physical protection and protective intelligence. To facilitate the detection of patterns of behavior in known would-be attackers, law enforcement agencies should implement information-sharing programs with other such organizations. Under most circumstances, law enforcement organizations are permitted to share such information. In many cases, law enforcement organizations can receive information, even though they may not provide information to other agencies. Other organizations and individuals often understand these restrictions and may be willing to give information that may help prevent attacks.



CHAPTER 4

Conducting a Threat Assessment Investigation



Opening a Case

An individual may come to the attention of protective intelligence professionals after exhibiting inappropriate or unusual interest in a protected person or by threatening a protected person. The information may be general (“I’m going to the State capital to even the score”) or specific (“John Smith wrote the mayor’s name on a .45 caliber bullet last night”). The person may be acting alone or as part of a group. Sometimes an individual is a person acting alone who becomes a fringe member of an extremist group, using the rhetoric and rationale of “the cause” for personal reasons.

Protective intelligence investigators determine whether the individual is already known to the unit and decide—using criteria identified during the program development phase—whether to initiate an investigation. If so, an investigator is assigned to begin an inquiry.

Inappropriate or unusual interest

Much of the information that initially comes to the attention of protective intelligence professionals appears on the surface to be relatively innocuous. When initial information (provided by either a suspected individual or another person) suggests that the suspected individual has an inappropriate or unusual interest in a protected person, it is reasonable to presume that the individual eventually will be deemed to not pose a threat. The investigator’s task is to search for information that rebuts this presumption and suggests that the individual does pose a real threat. Often, a relatively brief investigation will confirm that the individual has neither the interest, motive, nor means to mount an attack against a protected person, thus supporting the presumption that the individual is not a threat.

However, initial information sometimes suggests that the individual already has *taken action* on his or her inappropriate or unusual interest, such as going to the target’s home or office or approaching the target in a public place. The combination of

inappropriate or unusual interest coupled with *actions* based on that interest makes the case more serious.

In even more serious cases, the individual's actions involve weapons-seeking or weapons use. It is then reasonable to presume that the individual poses a real threat. Investigators of these persons should gather information refuting the assumption that the individual poses a threat, if such information is available or exists.

Threats

An individual may come to the attention of authorities after making a threat against a protected person or after being accused of making such a threat. Threats should always be taken seriously and investigated. Although many people who make threats against protected persons do not pose a real threat, some make threats in order to convey a warning that they are prepared to act. These individuals may interpret a lack of investigative interest in their threats as permission or encouragement to mount an attack.

Also, some people make threats against protected persons to signal that they are in danger of losing control and hurting someone. Making a threat is a way for them to get attention (albeit less direct than desirable) from authorities who they believe can prevent them from acting violently. Ignoring these threats might make the individual more desperate, possibly increasing the risk of violence to others, such as family members of the individual.

Occasionally, anonymous threats by phone, letter, or electronic mail come to the attention of law enforcement authorities. Individuals have various motives for communicating anonymous threats. ECSP information suggests that a few attackers and near-lethal approachers of prominent persons who made anonymous threats were trying to warn authorities that they were considering attacks. These individuals were ambivalent about attacking and were communicating with the hope that they might be stopped. Yet they did not want to identify themselves and make it more likely that the attack would be prevented.

Anonymous threats, though rarely acted upon, should be taken seriously and investigated to the fullest extent possible. Specific threats indicating that the threatener has plans to attack or that the threatener may have been in proximity to a protected person should be regarded with special concern.

Investigating a Case

Once a case has been opened, the protective intelligence investigator develops an investigation plan with the primary goal of collecting information and evidence that will help determine whether an individual has the interest, motive, and capacity to mount an attack on a target.

A protective intelligence investigation differs from other kinds of assessments of danger because the goal is to prevent a particular kind of violence: attacks directed against public officials or figures. For example, a parole board may try to assess the likelihood that an inmate, if released, will commit another crime. A mental health professional may attempt to predict whether a mentally ill person is likely to act violently if he or she is not hospitalized. These are different kinds of evaluations than the assessment required in a protective intelligence investigation.

Interviewing the subject

Traditionally, protective intelligence investigators have relied on their interview of the individual who is the focus of a protective intelligence investigation as a key (if not the key) source of information. But this rule is not ironclad—for example, if the subject is known to be a member of a radical or militant group, any interview should be considered only within the context of the overall strategy for investigating the group.

The timing of the interview is often a major question. It usually makes sense to first gather preliminary information about a subject's background and interests before conducting an interview, as background information can guide an investigator during the interview. Such background information may lead

the interviewer to areas relevant to whether the person poses a threat to particular targets.

Interviews can provide investigators with valuable information about subjects' thinking, motives for engaging in the behavior that initially brought them to the attention of the authorities, behavior that might be of concern, and leads for further investigation. Interviews may corroborate subjects' statements and be the basis for judging their veracity. Interviews also give subjects the opportunity to tell their personal stories, to be heard, and to reassess and redirect their behavior away from activities that concern investigators.

If at all possible, an interview should be conducted in a subject's "natural environment"—for example, at home—permitting the investigator to observe and gather nonverbal information and evidence that is relevant to the investigation, such as writings, pictures, and weapons that are within sight. Also, the investigator will learn about the subject's overall lifestyle and personality traits.

Investigators must sometimes interview persons who appear to be mentally ill. Such interviews often require special patience. Investigators should remember several basic principles regarding interviews with mentally ill subjects:

- Any subject, including a mentally ill subject, will behave in accord with how he or she perceives reality. Thus, to understand how a mentally ill subject has behaved or may behave in the future, investigators must learn how the person perceives reality. For example, a subject who believes that aliens are controlling his mind and telling him to attack the Governor may feel that he is being forced to stalk the Governor, even though he sees himself as generally law-abiding and knows that attacking the Governor is illegal. An investigator who dismisses this thinking as crazy, concluding that the subject is unlikely to act, and who stops the interview may not explore whether the subject has made efforts to get a weapon or travel to sites where the Governor is likely to be.

- People, including those who are mentally ill, are more likely to reveal their thoughts and actions when treated with respect. Mentally ill subjects who perceive their interviewers as interested in hearing what they have to say are more likely to tell their stories than those who feel humiliated or scorned.
- Someone who is acutely or chronically mentally ill may still be able to think clearly in some areas and to determine whether an investigator is speaking truthfully. Interviewers who use a style that is clear, direct, and nonjudgmental are more likely to solicit useful information than those using an approach in which they pretend to agree with a subject's delusions. An interviewer needs to be an active listener and to communicate a genuine interest in hearing and understanding the subject's story, no matter how outlandish it may seem. However, listening and understanding do not mean agreeing; an investigator should take care not to inadvertently reinforce the views of a delusional subject. Respectful skepticism will elicit more useful information: "I haven't had that experience, but I'm very interested in what you believe."

Although interviews can provide valuable information, relying too heavily on interviews does present problems. The information provided by the subject may be incomplete, misleading, or inaccurate. The interviewer may fail to solicit the information that is most relevant to the protective intelligence strategy called for in the investigation. The interviewee may present different information at different points in time, depending on his or her current circumstances, degree of desperation, mental health treatment, or other factors. In some cases, a subject's mental condition may be worsened by the interview.

Content of a protective intelligence investigation

Protective intelligence investigations differ from many other kinds of investigations in that the ultimate goal of these investigations is to prevent an attack, not to secure an arrest or conviction or to verify facts. Thus, any errors should be made on the side of safety and violence prevention.

Corroborated information and evidence. A primary task of a protective intelligence investigator is to seek and collect information and evidence to corroborate the statements of the subject of the investigation. Corroborated information about the individual's thinking and behavior facilitates assessment of the subject's interests, motives, and capacity to attempt to attack a protected person.

Corroborated evidence is more useful to investigators than subjective information and opinions. For instance, in a more traditional investigation, a detective would not ask a subject's wife, "Do you think he would ever pass a bogus check?" Likewise, asking the relative of a subject or a mental health professional questions such as "Do you think he is the type of person who would try to attack the mayor?" are rarely useful.

Areas of inquiry. A protective intelligence investigation of a subject should seek information in five areas:

The facts of the situation that initially brought the subject to the attention of the authorities. The first area of inquiry concerns how the subject came to the attention of the protective intelligence unit. In cases where the subject went to the mayor's office with "special information only for the mayor that will keep the city safe," the answer is obvious. But other situations may be less clear. For example, a threatening letter from the county jail to a judge signed John Doe, Inmate 502, may have been written by inmate Jones to get Doe into trouble. An anonymous call to the local police by a "concerned citizen" about Mary Smith's disparaging comments about the mayor and her recent purchase of a gun may be from a disgruntled employee who hopes to embarrass her by a visit from law enforcement agents. Providers of information may have multiple motives, and eyewitness accounts of people's behavior are notoriously inaccurate. Protective intelligence investigators should carefully establish the facts of a case to determine if the subject being reported is a victim and if the "informant" is the true threat.

General information about the subject. Three kinds of general information about a subject are gathered in a protective intelligence

investigation: identifiers, background information, and information about the subject's current life situation and circumstances.

- **Identifiers.** Identifying information (identifiers) includes the following:
 - Name and aliases.
 - Date of birth.
 - Social security and military identification numbers.
 - Current address.
 - Names and addresses of close relatives.
 - Physical description and current photograph.
 - Handwriting samples.
- **Background information.** Background information includes the following:
 - Education and training.
 - Criminal history.
 - History of violent behavior.
 - Military history.
 - History of expertise with and use of weapons.
 - Marital and relationship history.
 - Employment history.
 - Mental health history (especially involuntary psychiatric commitments, episodes of depression or despair, including suicidal thinking and behavior, and violent behavior while mentally ill).
 - History of grievances.
 - History of harassing others.
 - Interest in extremist ideas or radical groups.
 - Travel history, especially in the previous year.

There are four purposes for gathering background information: to learn about past behaviors, interests, and lifestyles of subjects that may influence their current interests, motives, or capacity to attempt an attack; to develop sources of information, if further inquiry into a subject's life (past and present) is needed; to develop information that could help investigators locate the subjects in the future; and to assist in managing cases that are deemed serious.

- **Current life situation and circumstances.** A third area of general information sought in protective intelligence investigations concerns the current living arrangements and environment of the subject being investigated. Inquiry about a person's current situation is based upon the knowledge that some persons engage in extreme behavior or reach out to law enforcement authorities when they are in transition, in crisis, or in an unstable living situation.

Protective intelligence investigators should consider a number of issues related to a subject's current situation. Is the subject in a stable living situation, with basic needs for food, clothing, shelter, and human contact being met? Is the subject currently employed, and how stable is the subject's employment situation? Is the subject currently or soon likely to be in transition or crisis? For example, has the subject recently left a marriage, job, or community? Will the subject soon be discharged from a correctional or mental health institution? How does the stability of the subject's current living situation compare with past living situations and with the subject's likely living situation in the near future? Does the subject appear to be on a downward course? For example, has the subject recently appeared to be giving up hope, becoming more desperate, losing important contacts and supports, or becoming suicidal? Who is the best source to identify and convey this information?

Information about attack-related behaviors. ECSP examinations of the thinking and behaviors of persons who have attacked or approached to attack prominent persons in the United States suggest that many attacks and near-lethal approaches are preceded by discernible attack-related behavior. This behavior is often observed by people in the subject's life; the protective intelligence

investigator who discovers such behavior in a subject will recognize it as a warning sign.

The idea that most assassins and near-lethal approachers engage in similar attack-related behaviors is consistent with an understanding of what is involved in mounting an attack on a protected person. An individual must select a target, locate the target, secure a weapon, travel to the vicinity of the target, and try to thwart whatever security measures are in place. These efforts may provide clues, indicating that the subject being investigated has been planning an attack. Protective intelligence investigators should look for evidence of attack-related behaviors, which can be categorized by whether or not weapons are involved.

Behaviors of concern in a threat assessment include:

- **An interest in assassination.** Manifestations of such an interest include gathering information about murder or assassination, writing to or about assassins, following news accounts of violence directed at public figures, visiting sites connected with assassinations, and emulating assassins.
- **Ideas and plans about attacking a public figure or official.** Evidence that a person has been thinking about or planning an attack may be revealed in comments to others, notes in a diary or journal, recent attention to the activities or travel of a public person, inquiries about law enforcement protective measures, travel patterns, attempts to breach security, or recent efforts to secure a weapon.
- **Communicating an inappropriate interest in a public official or figure, especially comments that express or imply an interest in attacking the person.** ECSP information suggests that attackers and near-lethal approachers rarely communicate direct threats to their targets or to law enforcement agencies, but many communicate information that indicates their intention to harm a target to relatives, coworkers, neighbors, or others.
- **Visiting a site linked to a protectee.** Appearance at an event or site where a public official or figure is, is believed to be, or

will be in the future is significant. Visits to these sites, when there is no obvious reason for the subject's appearance there, may be evidence of attack-related behavior.

- **Approaching a protectee.** To attack a protected person, an individual usually must travel to an event or site where the public official or figure is scheduled to be. Information that an individual has approached a target by visiting a site under these circumstances may be cause for concern.

Evidence of attack-related behavior involving a weapon should be taken very seriously by protective intelligence investigators. Of special interest is information about subjects purchasing or otherwise acquiring a weapon around the same time as they develop or hold an inappropriate or unusual interest in a public official or figure. In these circumstances, investigators must determine the intended use of the weapon.

Investigators should presume that an individual who has engaged in attack-related behavior involving a weapon or who has breached security is interested in attacking if given the opportunity. Investigative efforts in such a case should focus on ruling out the possibility of an attack. For example, investigators might establish that the individual had valid reasons, unrelated to a possible attack on a protected person, to carry a weapon or to travel to a certain site.

Motives. A thorough protective intelligence investigation involves careful attention to a subject's motives, because motives may determine whether a public official or figure is being targeted for attack and, if so, which persons are at greatest risk.

As noted in chapter 2, the 83 American assassins and near-lethal approachers studied by ECSP researchers had some combinations of eight motives. However, U.S. Secret Service case experience suggests that the motives of protective intelligence subjects who did *not* engage in near-lethal behavior have included the following:

- Bringing themselves to the attention of persons they perceived to be authorities.

- Instigating their involuntary commitment to a mental health or correctional institution.
- Effecting change in a current living situation viewed as intolerable (for example, to be moved from one prison to another).
- Obtaining help, e.g., being stopped from acting violently.
- Getting someone else in trouble.
- Obtaining attention or notoriety or bringing a concern to public attention.
- Achieving a special relationship with a public official or figure.
- Correcting a perceived wrong.
- Being injured or killed.

An investigator's opinion about the rationality of the subject's motives has no bearing on whether the subject will take action. Because subjects' acts are based on their perceptions of reality, the investigator's views will not determine a subject's future course of conduct. It may not matter whether the motives are illogical or rational, foolish or realistic, self-destructive or in the individual's best interests.

For example, a subject who believes that she is a relative of a public figure and that she has been invited to move into the public figure's residence is unlikely to be dissuaded by an investigator's rational analysis. Such a person is likely to continue to believe that she is related to the public figure despite facts to the contrary. The interviewer's tasks in such a case are to understand how the subject views her situation, not to reinforce any delusional ideas, and to try to gauge what action the subject might take based on her perceptions and beliefs.

The motive of suicide can also be a factor in near-lethal approaches or attacks on public figures and officials. This phenomenon—"suicide by cop"—has received considerable attention in the past 10 years. An individual who wants to die, but is not willing or able to take his or her own life, may believe that instigating gunfire by approaching a protected person with a weapon is a way to get killed.

When coupled with an individual's wish for fame or notoriety, suicide becomes an even more ominous motive. An individual whose motives are notoriety and suicide may consider attacking a political leader, even though he or she has no political interest and no negative feelings about the protected person. The only issue that matters is that the public official is protected by armed law enforcement officers and will be accompanied by news media that will record the assailant's death.

Target selection. Many attackers and near-lethal approachers may consider *several* potential targets and change their primary target several times.

For example, the published diary of Arthur Bremer (who shot Alabama Governor George Wallace in 1972) suggests that his first target was President Richard Nixon. After unsuccessfully attempting to position himself to shoot the President during a trip to Ottawa, Canada, Bremer shifted his interest to Wallace, by then a Presidential candidate. Other near-lethal attackers have shifted from one target to another based on their perception of the importance of a given target. One subject shifted between attacking a Governor, a Senator, and a Presidential candidate, settling on the candidate because he thought a "Presidential candidate is much more powerful."

When gathering information, therefore, investigators should be alert to the possibility that a subject has considered, is simultaneously considering, or might consider in the future a number of public officials or figures as possible targets. Selection of a primary target may depend on many factors, such as the subject's motives, ability to travel, financial situation, and opportunities to approach a target, as well as the perceived importance of, the media attention given to, and the perceived security afforded a target.



CHAPTER 5

Evaluating a Threat Assessment Case



A protective intelligence investigation, at least in part, is an effort to predict specific future violence. Two points about violence prediction are worth consideration. First, violence prediction is conditional—not a yes-no, “this person will be violent or will never be violent” proposition. A prediction of violence is a statement that, given certain circumstances or conditions, a specified risk exists that a particular subject will act violently toward a particular target.

Second, targeted violence is different than other kinds of violence, and attacks on public officials or figures appear to be a specific kind of targeted violence. An attack on a mayor, Governor, or President is a different kind of behavior than an armed robbery, rape, or attack on a roommate. A murder of a celebrity or a business leader is a different kind of violence than a murder of a parent or neighbor. ECSP information about attackers and would-be attackers of prominent persons suggests that some factors that have been seen as general predictors of violence, such as a history of violence, may not specifically predict violence toward a public official or figure.

Principles to Guide a Protective Intelligence Evaluation

After information about a subject has been gathered, this material must be organized and evaluated. A two-stage process is suggested. First, information should be examined for evidence of behavior and conditions that would be consistent with the likelihood of a violent attack on a public person. In the second stage of evaluation, the protective intelligence investigator will determine whether a subject appears to be moving toward an attack and, if so, how rapidly.

Protective intelligence investigators should conduct threat assessments using two principles discussed in chapter 2 as guides:

- Assassination is the result of an understandable and often discernible process of thinking and behavior.

- Assassination stems from an interaction of the potential attacker, event, situation, and target.

Questions to Ask in a Threat Assessment

Investigators should ask a number of questions of both the subject and collateral sources throughout the investigation. The answers to these questions will guide the evaluation:

- What motivated the subject to make the statement or take the action that caused him or her to come to attention?
- What, if anything, has the subject communicated to someone else (target, law enforcement, family, friends, colleagues, associates) or written in a diary or journal concerning his or her intentions?
- Has the subject shown an interest in any of the following?
 - Assassins or assassination.
 - Weapons (including recent acquisition of a weapon).
 - Militant or radical ideas/groups.
 - Murders, murderers, mass murderers, and workplace violence and stalking incidents.
- Is there evidence that the subject has engaged in menacing, harassing, and/or stalking-type behaviors? Has the subject engaged in attack-related behaviors? These behaviors combine an inappropriate interest with any of the following:
 - Developing an attack idea or plan.
 - Approaching, visiting, and/or following the target.
 - Approaching, visiting, and/or following the target with a weapon.
 - Attempting to circumvent security.
 - Assaulting or attempting to assault a target.

- Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, etc., with indications that the subject has acted on those beliefs?
- How organized is the subject? Does the subject have the ability to plan and execute a violent action against a target?
- Is there evidence that the subject is experiencing desperation and/or despair? Has the subject experienced a recent personal loss and/or loss of status? Is the subject now, or has the subject ever been, suicidal?
- Is the subject's "story" consistent with his or her actions?
- Are those who know the subject concerned that he or she might take action based on inappropriate ideas?
- What factors in the subject's life and/or environment might increase or decrease the likelihood that the subject will attempt to attack a target (or targets)?

In addition, an investigator should address troubling or unresolved issues about a particular case, which could include missing information or new information that might clarify the subject's motives and interests.

Attacks on public officials and figures are rare; all cases that are serious enough to be opened deserve a thorough investigation. Usually, information gathered during the investigation will lead to the conclusion that the subject does not pose a threat. However, sometimes the facts cause the investigator to become concerned about the risk a subject poses. These cases require particularly painstaking investigative efforts and consideration.

In most cases, an investigator should consult with other professionals before drawing a conclusion about whether a subject poses a threat to a public official or figure. Another investigator with protective intelligence experience is often the most effective consultant. However, people with special expertise that might pertain to the facts of a given case can sometimes offer a useful

perspective. For example, a mental health professional who has experience assessing mentally ill persons who act violently and who is familiar with the operations of law enforcement agencies could help assess information about a mentally ill subject.

Documenting and keeping a record of the information gathered and evaluated in a protective intelligence investigation is vital. A well-documented record permits others to review the case and offer assistance, and shows that the investigation was performed with care and attention. Also, a carefully documented case file provides baseline information about a subject's thinking and actions at a certain point in time, which can be invaluable if the subject is investigated again or if future investigators need to determine whether the subject has changed thought or behavior patterns.

Protection

Those charged with protection of the targeted public official or figure must be notified about cases of concern, and the information should be incorporated into protection activities. The structure and operations of an organization should determine how threat assessment data are connected to protection activities. For instance, if an organization has one unit responsible for protection and one for threat assessment functions, this often can be accomplished through intramural briefings. Briefing of protectors usually includes a description of a subject's identifiers, behavior, interests, and current location and situation. However, such briefings should be two-way exchanges of information, because protectors often have information that can be important in a protective intelligence investigation as well as in followup investigations used in monitoring the subject.



CHAPTER *6*

Managing a Protective Intelligence Case



In most protective intelligence cases, based on the information gathered, investigators determine that an individual does not pose a risk to a public person. The majority of these cases are closed following the investigation, unless a criminal violation occurred (for example, the subject threatened a public official) or protectors feel that the subject may harm a person other than the original target. If a criminal violation has occurred, the case may be presented to the prosecutor's office for possible charges. If investigators believe that a subject is a threat to an unprotected person, they can attempt to direct the subject to the appropriate resources or otherwise intervene to prevent violence.

When a thorough investigation suggests that the subject has the interest, motive, and ability to attempt an attack on a public official or figure, the investigator's task is to manage the case so that violence does not occur. Successful case management involves considerable time and effort and is composed of two functions: efforts directed at protection (discussed in chapter 5), so that a target is shielded from the potential assailant, and efforts directed at monitoring, controlling, and redirecting the subject.

Monitoring, Controlling, and Redirecting the Subject

The central premise of case management efforts is that violence directed against a protected person is in no one's best interest, including that of the potential assailant. Coordinated, consistent efforts to tell the potential attacker that an attack will not be permitted and that it is not in anyone's best interest to attack can increase the chance that a subject will abandon the idea of assassination.

Unless there is reason to do otherwise, the subject should be made aware of the investigation and told that unacceptable interest in a protected person and unacceptable behavior must change. This message should be communicated to the subject clearly and professionally. However, in certain investigations—for example, those involving a member of a radical or militant group—it may not be appropriate to alert the subject.

Many people considered a threat want attention and will accept ongoing contact with the law enforcement or security organization responsible for protective intelligence. Therefore, the subject should be asked to cooperate with being monitored by the investigator and the law enforcement or security agency. For example, the agency might ask the subject to report all planned travel and to check in with the investigator on a regular basis.

Many subjects see law enforcement officers as important authority figures in their lives. Regular, respectful interviews, in which investigators listen while delivering a consistent, clear message about unacceptable behavior, are key to supporting these subjects as they attempt to change. For a mentally ill subject, simply reinforcing the idea that he or she must remain connected to and cooperative with mental health treatment professionals may be sufficient. Other cases, such as those involving terrorists, call for different strategies.

Effective case management is aided by a systems perspective. That is, investigators should identify existing social systems that might help them manage persons who are potential threats. Social systems that might work cooperatively with the investigator to engage, neutralize, and redirect the potential attacker include the following:

- Criminal justice system (prosecutors, courts, probation officers, correctional officials).
- Health and mental health care organizations (managed care organizations, public mental health agencies, local hospitals).
- Social services organizations.
- Religious organizations to which the subject belongs or in which the subject is interested.
- Community organizations.
- Family and friends.

Ending Monitoring

The purpose of connecting the subject to services and systems that will aid and encourage change is ultimately to enable the investigator to discontinue monitoring. After monitoring is ended and a case is closed, the subject may continue to be involved with service systems that aid successful functioning.

The investigator will be able to end monitoring after performing the following tasks:

- Assessing whether (and to what extent) the subject has changed unacceptable thinking and behavior over time.
- Developing and supporting intervention strategies that encourage and help the subject to change.

Sources of postassessment information

To evaluate changes in behavior, an investigator should develop a baseline of the subject's behaviors of concern and then collect information over time about the subject from multiple and consistent sources. Such a strategy takes into account the likelihood that the living conditions may change, as may the law enforcement or security staff with responsibility for ongoing investigation of the subject.

To permit later comparisons to baseline behavior, the investigator should write detailed descriptions of the subject's initial attack-related behavior and worrisome thinking and actions when he or she was first deemed a threat. A list also should be compiled of persons and organizations who can be contacted at regular intervals for information about the subject's behavior. Collateral-source information can corroborate or clarify information gained directly from interviews with a subject during the case management process. An interview with such a subject might be followed by interviews with others who are in regular contact with the subject to determine whether he or she behaves in a manner consistent with his or her statements to the investigator. For example, a prison inmate who tells an investigator that he is no longer interested in the Governor but who is described

by the shift commander on the cell block as being intensely interested each time the Governor appears on the news might be suspect in other comments about his interests and behaviors. Similarly, seeking an opinion from a doctor in a mental health unit who has little contact with a subject about the likelihood that the patient will try to kill the Governor may prove less useful than interviewing a mental health worker who frequently interacts with the patient.

Closing a Case

A protective intelligence investigator can close a case when he or she is able to:

- Articulate why a subject was originally considered to pose a threat.
- Document changes in the subject's thinking and behavior that negate the original concerns.
- Describe why the subject is unlikely to pose a future threat to protected persons.

If postassessment contacts have been made, closing the case involves ensuring that the subject understands that the protective intelligence investigator will initiate no further contact. For some subjects, cessation of contact with the investigator may be a desired goal and a relief; for others, the thought of ending contact with officials who they viewed as helping them may be difficult. In most cases, therefore, it makes sense that discontinuance of contact be gradual, rather than abrupt. Ongoing contact with other organizations, such as mental health or social services agencies, can help these subjects function after their contact with the law enforcement or security organization has ended.

Conclusion

The ECSP has developed knowledge about assassins, attackers, and near-lethal approachers and about other forms of targeted violence. This guide has incorporated this information and is offered as an aid for law enforcement agencies and other organi-

zations to formulate their own processes and protocols for investigating, evaluating, and managing people who are considered threats to public officials and figures.

The ECSP underscores an important point: Nearly all citizens of the United States share the task of preventing assassinations and attacks—physical protection and protective intelligence are not just the responsibility of law enforcement and security organizations. The public, other law enforcement and security organizations, mental health and social services agencies, the private sector, and the media can help identify, assess, and manage potential attackers and thus help to prevent attacks and assassinations.

Notes

1. Fein, Robert A., and Bryan Vossekuil, *Preventing Assassination: Secret Service Exceptional Case Study Project*, unpublished report, Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, and U.S. Department of the Treasury, U.S. Secret Service, 1997.

2. A near-lethal approacher is defined here as an individual who exhibits behaviors that suggest he or she is preparing for an attack on another person and who, without intervention, might attack. Such behaviors include acquiring a weapon and traveling to a site where the target is believed to be. An attacker is a person who actually mounts an attack, while an assassin is a successful attacker.

To find out more information about the National Institute of Justice,
please contact:

National Criminal Justice Reference Service
Box 6000
Rockville, MD 20849-6000
800-851-3420
e-mail: askncjrs@ncjrs.org

To obtain an electronic version of this document, access the NIJ Web site
(<http://www.ojp.usdoj.gov/nij>).

If you have any questions, call or e-mail NCJRS.

About the National Institute of Justice

The National Institute of Justice (NIJ), a component of the Office of Justice Programs, is the research agency of the U.S. Department of Justice. Created by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, NIJ is authorized to support research, evaluation, and demonstration programs, development of technology, and both national and international information dissemination. Specific mandates of the Act direct NIJ to:

- Sponsor special projects and research and development programs that will improve and strengthen the criminal justice system and reduce or prevent crime.
- Conduct national demonstration projects that employ innovative or promising approaches for improving criminal justice.
- Develop new technologies to fight crime and improve criminal justice.
- Evaluate the effectiveness of criminal justice programs and identify programs that promise to be successful if continued or repeated.
- Recommend actions that can be taken by Federal, State, and local governments as well as by private organizations to improve criminal justice.
- Carry out research on criminal behavior.
- Develop new methods of crime prevention and reduction of crime and delinquency.

In recent years, NIJ has greatly expanded its initiatives, the result of the Violent Crime Control and Law Enforcement Act of 1994 (the Crime Act), partnerships with other Federal agencies and private foundations, advances in technology, and a new international focus. Some examples of these new initiatives:

- Exploring key issues in community policing, violence against women, violence within the family, sentencing reforms, and specialized courts such as drug courts.
- Developing dual-use technologies to support national defense and local law enforcement needs.
- Establishing four regional National Law Enforcement and Corrections Technology Centers and a Border Research and Technology Center.
- Strengthening NIJ's links with the international community through participation in the United Nations network of criminological institutes, the U.N. Criminal Justice Information Network, UNOJUST (United Nations Online Justice Clearinghouse), and the NIJ International Center.
- Improving the online capability of NIJ's criminal justice information clearinghouse.
- Establishing the ADAM (Arrestee Drug Abuse Monitoring) program—formerly the Drug Use Forecasting (DUF) program—to increase the number of drug-testing sites and study drug-related crime.

The Institute Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the Department of Justice, and the needs of the criminal justice field. The Institute actively solicits the views of criminal justice professionals and researchers in the continuing search for answers that inform public policymaking in crime and justice.

OFFICE OF COURT SECURITY SERVICES
STAFFING GUIDELINES
COURTS OUTSIDE NEW YORK CITY

I. SMALL COUNTIES (MULTI-HAT)

1. A minimum of one full-time security position for each court operation.
2. One security position for each additional judge over the first.
3. One security position for each Family Court Hearing Examiner.
4. One part-time or per-diem security position for each visiting judge.
5. Additional security positions to provide building security where justified.

II. CITY COURTS (SMALL JURISDICTIONS)

1. A minimum of one full-time security position for each court operation.
2. One part-time or per-diem security position for each part-time judge over the first.
3. Additional security positions to provide building security where justified.

III. LARGE COUNTIES AND CITIES - (Erie, Monroe, Onondaga, Buffalo, Rochester and Syracuse)

1. One security position for each Civil Part.
2. Two security positions for each Criminal Part.
3. Two security positions for each Family Court Part.
4. One security position for each Family court Hearing Examiner Part.
5. Two security positions for each City Court Part.
6. Additional security positions to provide building security where justified.

IV. NASSAU, SUFFOLK and WESTCHESTER COUNTIES

A. DISTRICT COURT - (Nassau and Suffolk Counties)

1. Three court officers for each criminal part.
2. One court officer for each civil part.
3. Two court officers for each outlying court facility.
4. Six court officers for each arraignment part.
5. Seven court officers for each night court arraignment.
6. One court officer for each floor in which parts or chambers are located.
7. Seven court officers for each weekend court arraignment.
8. One Court Officer/Sergeant for every six Court Officers.
9. Unique security posts where justified.
10. A 10% coverage factor to allow for vacations, illness and other absences applied to those positions not assigned to parts with the exception of Arraignment parts.

11. One Principal Court Officer.
12. One Associate Court Officer for each court that has more than one location which has five or more regularly scheduled parts, or which has fifty or more officers assigned to a single location.
13. One Assistant (Court Officer/Sergeant) for each Principal or Associate Court Officer, with a maximum of one per facility. NOTE: In those counties where there are earmarked Security Supervisors or Supervising Court Officers, those Supervisors will be assigned as Assistants in lieu of Court Officer/Sergeants.

B. FAMILY COURT

1. Two Court Officers for each Family Court Part.
2. One Court Officer for each Hearing Examiner Part.
3. One Court Officer for each floor in which parts or chambers are located.
4. Unique security posts where justified.
5. A 10% coverage factor to allow for vacations, illness and other absences.
6. One Principal Court Officer.
7. One Associate Court Officer for each court that has more than one location, which has five or more regularly scheduled parts, or which has fifty or more officers assigned to a single location.
8. One Court Officer/Sergeant for each Family Court facility, in lieu of one of the Court Officers in Paragraphs 1 through 4.
9. One Assistant (Court Officer/Sergeant for each Principal or Associate Court Officer with a maximum of one per facility. NOTE: In those counties where there are earmarked Security Supervisors or Supervising Court Officers, those Supervisors will be assigned as Assistants in lieu of Court Officer/Sergeants.

39

10

370

OFFICE OF COURT SECURITY SERVICES
STAFFING GUIDELINES
NEW YORK CITY COURTS

I. CIVIL COURT

1. One Court Officer for each Calendar Part.
2. One Court Officer for each Trial Part.
3. Three Court Officers for each Housing Calendar Part.
4. One Court Officer for each Housing Trial Part.
5. Three Court Officers, and one Court Officer/Sergeant for each Small Claims night court operations.
6. One Court Officer for each floor on which parts or chambers are located.
7. One Court Officer/Sergeant for each county (excluding Richmond), in lieu of one of the Court Officers in Paragraphs 1 through 4.
8. Unique security posts where justified.
9. A coverage factor of 10% to allow for vacations, illness and other absences applied to all positions.
10. One Associate Court Officer for each court location which has five or more regularly scheduled parts.
11. One Principal Court Officer for the citywide operation
12. One Assistant (Court Officer/Sergeant) for each Associate Court Officer, and one Assistant (Court Officer/Sergeant) for each Principal Court Officer (Citywide operation).
13. One Court Officer/Sergeant for Richmond County, who will act as the Officer-In-Charge.

III. CRIMINAL COURT

1. Five Court Officers and one Court Officer/Sergeant for each Day Arraignment Part.
2. Ten Court Officers and one Court Officer/Sergeant for each Night Arraignment Part.
3. 2.5 Court Officers for each Jury Part, and one Court Officer/Sergeant for every two jury parts.
4. Five Court Officers, and one Court Officer/Sergeant for each All Purpose Part.
5. Five Court Officers, and one Court Officer/Sergeant for each Summons Arraignment Part.
6. One Court Officer/Sergeant for each lobby magnetometer operation.
7. One court officer for each floor in which parts or chambers are located.
8. Unique security posts where justified.
9. A 10% coverage factor to allow for vacations, illness and other absences applied to those positions not assigned to parts, with the exception of Night Arraignment Parts.
10. One Associate Court Officer for each court location which has five or more regularly scheduled parts.
11. One Principal Court Officer for the citywide operation.
12. One Assistant (Court Officer/Sergeant) for each Associate Court Officer, and one Assistant (Court Officer/Sergeant) for each Principal Court Officer (Citywide operation).
13. One Court Officer/Sergeant for Richmond County who will act as the Officer-In-Charge.

C. SUPREME AND COUNTY COURT

1. Three Senior Court Officers and one Court Officer/Sergeant for each criminal part.
2. One Senior Court Officer for each civil part.
3. One Senior Court Officer for every four full-time Judicial Hearing Officers.
4. One Senior Court Officer for each floor in which parts or chambers are located.
5. Unique security posts where justified.
6. A 10% coverage factor to allow for vacations, illness and other absences applied to all positions with the exceptions of criminal parts.
7. One Principal Court Officer for each court.
8. One Associate Court Officer for each court that has more than one location which has five or more regularly scheduled parts, or which has fifty or more officers assigned to a single location.
9. One Assistant (Senior Court Officer/Sergeant) for each Principal or Associate Court Officer with a maximum of one per facility. NOTE: In those counties where there are earmarked Security Supervisors or Supervising Court Officers, those Supervisors will be assigned as Assistants in lieu of Senior Court Officer/Sergeants.

D. MAGNETOMETER OPERATIONS

1. Floor Security: Where magnetometers are placed on individual floors. Two officers assigned to each magnetometer. (Note:) the two officers are replacements, not in addition to the officers assigned non-courtroom posts on the floor.
2. Lobby Security: Two court officers for each magnetometer with the addition of one officer for each building entrance.
3. A 10% coverage factor to allow for vacations, illness and other absences, applied to all the above positions.

V. ALL OTHER COUNTIES

1. A minimum of one full time security position for each court operation.
2. Up to 1.5 security positions for each Criminal part.
3. Up to 1.5 security positions for each Family Court part.
4. One security position for each Family Court Hearing Examiner.
5. One security position for each Civil part.
6. Additional security positions to provide building security where justified.

VI. ALL OTHER CITIES

1. A minimum of one full time security position for each court operation.
2. Up to 1.5 security positions for each additional judge over the first.
3. Additional security positions to provide building security where justified.

II. FAMILY COURT

1. Two Court Officers for each All Purpose part.
2. Three Court Officers for the Centralized Foster Care Part.
3. Four Court Officers for the Designated Felony and Child Abuse Part.
4. One Court Officer for each Intake part (Note:) The judge sitting in the intake part is always rotated from another part, leaving that part idle. The officers assigned to that judge will be in addition to the staff allocated to this part.
5. One Court Officer for each Hearing Examiner.
6. One Court Officer for each waiting room.
7. One Court Officer for each floor in which parts or chambers are located.
8. One Court Officer/Sergeant for the centralized Child Support Enforcement Term (New York County).
9. Two Court Officer/Sergeants for each county (excluding Richmond), in lieu of two of the Court Officers in Paragraphs 1 through 5.
10. Unique security posts where justified.
11. A coverage factor of 10% to allow for vacations, illness and other absences applied to all positions with the exception of Designated Felony and Child Abuse Parts.
12. One Associate Court Officer for each court location which has five or more regularly scheduled parts.
13. One Principal Court Officer for the citywide operation.
14. One Assistant (Court Officer/Sergeant) for each Associate Court Officer, and one Assistant (Court Officer/Sergeant) for each Principal Court Officer (Citywide operation).
15. One Court Officer/Sergeant for Richmond County who will act as the Officer-In-Charge.

IV. SUPREME COURT

1. Three Senior Court Officers, and one Senior Court Officer/Sergeant for each Criminal Part.
 2. One Senior Court Officer for each Civil Part.
 3. Four Senior Court Officers, and one Senior Court Officer/Sergeant for each Arraignment or Conference Part.
 4. One Senior Court Officer/Sergeant for each facility in the Civil Branch of the Supreme Court, 1st Department.
 5. Two Senior Court Officers for each Grand Jury Complex.
 6. One Senior Court Officer for each County Clerks Office.
 7. One Senior Court Officer for every four full time Judicial Hearing Officers.
 8. One Senior Court Officer for each floor in which parts or chambers are located.
 9. Unique security posts where justified.
 10. A 10% coverage factor to allow for vacations, illness and other absences applied to all positions with exceptions of Criminal Parts.
 11. One Principal Court Officer for each criminal and civil term of the Supreme Court in the four major counties of New York City.
 12. One Associate Court Officer for each court that has more than one location, which has five or more regularly scheduled parts, or which has fifty or more officers assigned to a single location.
 13. One Assistant (Senior Court Officer/Sergeant) for each Principal or Associate Court Officer with a maximum of one per facility.
- NOTE: In those counties where there are earmarked Security Supervisors or Supervising Court Officers, those Supervisors will be assigned as Assistants in lieu of Senior Court Officers/Sergeants.

V. SURROGATE'S COURT

1. One officer assigned to each Surrogate
2. Unique security posts where justified

VI. MAGNETOMETER OPERATIONS

1. Floor Security: Where magnetometers are placed on individual floors. Two officers assigned to each magnetometer. (Note:) the two officers are replacements, not in addition to the officers assigned non-courtroom posts on the floor.
2. Lobby Security: Two court officers for each magnetometer with the addition of one officer for each building entrance.
3. A 10% coverage factor to allow for vacations, illness and other absences, applied to all the above positions.

APPENDIX B

SAMPLE COURT ORDER FOR SEQUESTERED JURIES

THE SUPRIOER COURT OF THE STATE OF _____
IN AND FOR THE COUNTY OF _____

PEOPLE OF THE STATE OF _____

v.

CRIMINAL NO. _____

ORDER

It is hereby ORDERED this _____ day of _____, 20____, that the jurors and alternate jurors in this case shall be sequestered and shall thereafter be kept in the custody of the Sheriff of _____ County for the duration of this trial, or until further notice from this Court.

It is further ORDERED as follows:

1. The Sheriff shall make arrangements for appropriate accommodations for the jury during the trial, and shall provide for adequate security in the jurors' quarters beginning _____ day of _____.
2. The Sheriff shall make satisfactory arrangements to assist the jurors in securing apparel and personal items from their homes.
3. The Sheriff shall make appropriate arrangements for the furnishing of vehicles (including the hiring of vehicles, if necessary) for the transportation of jurors between their place of lodging and the County Courthouse.
4. During the period of sequestration, the Sheriff shall provide to each of the jurors and alternate jurors so sequestered, breakfast, lunch and dinner, a maximum of two cocktails during, or following, the evening meal (dinner) if they are not to return to the Courthouse following the meal.
5. The Sheriff shall maintain appropriate records during the trial providing:
 - a. A record of deputies' assignments to shifts and duty stations;
 - b. A record of jurors' quarters;
 - c. A record of persons entering the area of jurors' quarters; and
 - d. A record of telephone calls to and from the jurors' quarters.The assigned Sheriff's personnel shall make certain that no member of the jury:
 - a. Has any unauthorized contract with any outside person;
 - b. Reads newspapers, magazines, periodicals or listens to radio or television newscasts or bulletins pertaining to the trial or programs where the them resembles the case being heard or decided upon;

- c. Has any discussion with any outside person pertaining to the case;
 - d. Has any discussion of the case with other jurors before the case is submitted for deliberation;
 - e. Has written or telephone communication with any person, except under the direct supervision of the assigned Deputy Sheriff, on matters not pertaining to the case; and/or
 - f. Any communication with the Court shall be made in writing and placed in a sealed envelope by the jury or individual juror, and upon being turned over the sheriff's personnel will be promptly delivered to the Court.
- 6. The Sheriff shall make appropriate arrangements for suitable recreation for the jury.
 - 7. Mail and packages, to and from jurors, shall be censored to ensure that no information relative to the trial is transmitted.
 - 8. The Sheriff shall make arrangements to provide, at county expense, a nonalcoholic beverage (coffee, tea, milk, soda) on court days during the morning and afternoon recess, and also at the place of lodging after the evening meal.
 - 9. The Sheriff, if necessary, shall provide laundry service to the jurors at county expense.
 - 10. The Sheriff shall make provisions to transport any juror who has previously made such arrangement with the court to such medical doctors whose names the jurors shall furnish to the Sheriff.
 - 11. The Sheriff shall make provisions for the videotaping of television programs which will subsequently shown to the jurors, thereby eliminating the possibility of hearing or seeing news bulletins.
 - 12. The Sheriff shall, to the extent feasible, make suitable arrangements for jurors to attend religious services if such arrangement can be made under custodial supervision.
 - 13. The Sheriff shall make satisfactory arrangements for barber shop and/or beauty salon services for the jurors, but always under proper custodial supervision.
 - 14. The Sheriff shall make provisions at county expense for recreational activities of the jurors, including: attendance at athletic events, theater, picnics and short trips for dining purposes or to historical or scenic sites where overnight travel is not involved.
 - 15. This Order may be altered, amended and/or changed from time to time as in the Court's judgment conditions warrant.

Judge of the Superior Court