CCJ/COSCA
Court Security Handbook

Ten Essential Elements for Court Security and Emergency Preparedness

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

Conference of Chief Justices

COSCA
Conference of State Court Administrators

CCJ/COSCA
Court Security Handbook

Ten Essential Elements for Court Security and Emergency Preparedness

JUNE 2010

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

Conference of Chief Justices

COSCA
Conference of State Court Administrators

Table of Contents

Appendices

Dedication

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

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

Acknowledgements

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

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

Members of the Committee in fiscal year 2009-2010 are:

CCJ Members	**COSCA Members**
Thomas J. Moyer (dec.), OH, ***Co-Chair***	Zygmont A. Pines, PA, ***Co-Chair***
Sharon Keller, TX, ***Co-Vice Chair***	Karl R. Hade, VA, ***Co-Vice Chair***
Sue Bell Cobb, AL	Joseph Baxter, RI
James E. Edmondson, OK	Steven D. Canterbury, WV
Thomas R. Fitzgerald, IL	James T. Glessner, ME
Paul A. Suttell, RI	Elisabeth H. Goodner, FL
Barton R. Voigt, WY	Donald D. Goodnow, NH
	Glenda L. Lake, VI
	Arthur W. Pepin, NM
	A. John Voelker, WI
	Anne B. Wicks, DC

We would also like to offer special thanks to our many colleagues, consultants, and court experts for their comments and contributions to the ten chapters contained in this handbook. Those who contributed greatly to the development and publication of this report are reviewers of the handbook — Steve Canterbury, Lisa Goodner, and Pat Griffin as well as NCSC liaison to the Committee, Timothy Fautsko, and former liaisons Carolyn Ortwein and José Dimas. Other contributors are Judy Amidon, Steve Berson, Ephanie

Blair, Pam Casey, Tom Clarke, Paul Embley, Kay Farley, Dan Hall, Laura Klaversma, Frank Lalley, Arnold Lum, Jim O'Neil, Kevin Sheehan, Jewel Williams, [Note: additional names will be added before publication with committee approval.]

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

Essential Ten Elements for Effective Courtroom Safety and Security Planning

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

1. Operational Security: Standard Operating Procedures

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

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

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

3. Emergency Preparedness and Response: Continuity of Operations

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

4. Disaster Recovery: Essential Elements of a Plan

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

5. Threat Assessment

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

6. Incident Reporting

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

7. Funding

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

8. Security Equipment and Costs

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

9. Resources and Partnerships

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

10. New Courthouse Design

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

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

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

Introduction

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

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

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

Element 1 - Operational Security: Standard Operating Procedures

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

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

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

Element 3 - Emergency Preparedness and Response: Continuity of Operations

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

Element 4 - Disaster Recovery: Essential Elements of a Plan

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

Element 5 - Threat Assessment

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

Element 6 - Incident Reporting

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

Element 7 - Funding

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

Element 8 - Security Equipment and Costs

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

Element 9 - Resources and Partnerships

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

Element 10 - New Courthouse Design

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

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

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

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

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

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

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

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

EMERGENCY MANAGEMENT for COURTS
Strategies for Success

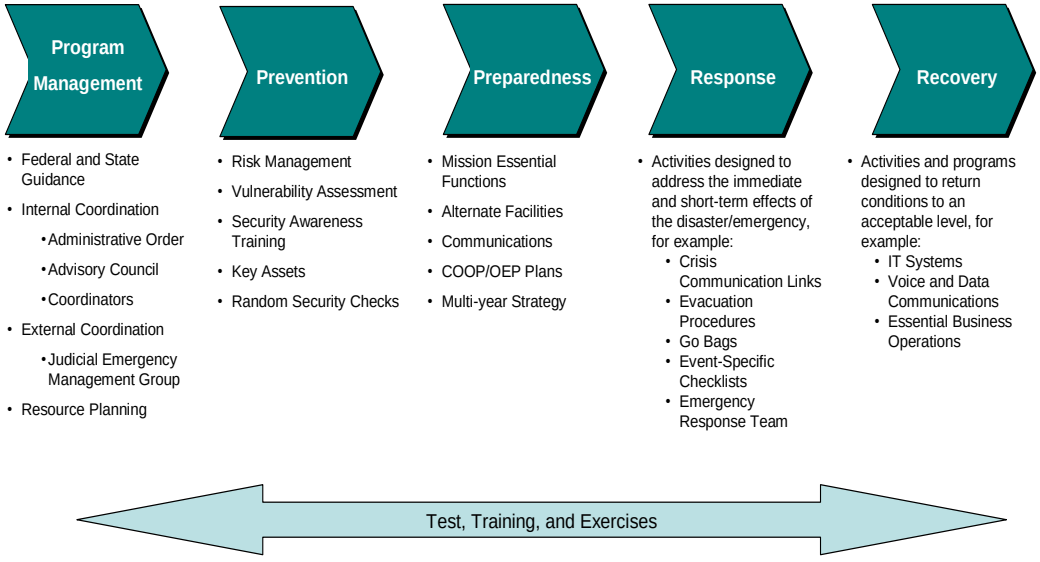
The following illustrates the steps needed for the development of comprehensive security and emergency preparedness programs for state and local courts.

Strategy for a Comprehensive Emergency Preparedness Program

Vision

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

Emergency Preparedness Program Elements



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

NCSC *Best Practices Institute*

Emergency Management for Courts

Overview

Emergency management[1] is critical to court performance. For many years, court leaders have been concerned with ensuring the safety of all who use the nation's courthouses. During the 1978 Second National Conference on the Judiciary, participants recognized that "security in the courtroom and in the courthouse has been an increasing problem in recent years" (Friesen, 1978, p. 195). The 1990 *Trial Court Performance Standards* required courts to ensure the safety of their facilities (Commission on Trial Court Performance Standards, 1990). In 1995, the National Association for Court Management produced the *Court Security Guide*, and several states followed with their own security manuals.

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

References

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

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

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

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

Why Develop Emergency Management Best Practices?

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

How Were The Practices Developed?

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

What Does Court Emergency Management Include?

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

What Are the Best Practices?

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

1. Ensure visible court leadership.

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

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

Examples

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

Resources

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

2. Survey and prioritize emergency management needs.

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

Examples

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

Resources

- ✔ "Court Security Manual." State of Minnesota & Conference of Chief Justices, 1997. *(See security checklist beginning on p. 2-3-1.)* http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/MinnesotaCtSecurityManual.pdf
- ✔ "Court Security Incident Reporting Form." Minnesota Department of Public Safety, Bureau of Criminal Apprehension, 1993. *(Provides an example of an incident reporting form.)* http://www.dps.state.mn.us/bca/Forms/Documents/court-incid.pdf
- ✔ "Measure 1.2.1: Courthouse Security Audit." Commission on Trial Court Performance Standards, 1995. *(Includes National Sheriffs' Association Physical Security Checklist.)*. http://www.ncsconline.org/D_Research/TCPS/Standards/stan_1.2.htm
- ✔ United States Marshals Service. *(Includes address and telephone numbers of district offices.)* http://www.usdoj.gov/marshals/usmsofc.html

3. Create and practice an emergency response plan.

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

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

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

Examples

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

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

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

Resources

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

4. Get a seat at the table.

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

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

Examples

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

Resources

- ✔ "Communication is Key in Court Security." Amanda Murer, Report on Trends in the State Courts, National Center for State Courts, 2002. *(Touches on the importance of communication with others in community when making a security plan. Also gives ideas of how to improve court security plan without monetary support.)* http://www.ncsconline.org/D_KIS/Trends/Trends02MainPage.html
- ✔ "Emergency Management Guide for Business & Industry." FEMA, pgs. 39-40. *(Discusses emergency planning with other community agencies.)* http://www.fema.gov/pdf/library/bizindst.pdf
- ✔ Homeland Security Contact List. Whitehouse Web site: http://www.whitehouse.gov/homeland/contactmap.html
- ✔ "Keep the Courts Open." Final report of the Florida Supreme Court Workgroup on Emergency Preparedness, March 28, 2002. *(Discusses the importance of communication and cooperation in planning for responses to threats and emergencies.)* http://www.9-11summit.org/ materials911/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/Florida FinalReport.pdf
- ✔ Office of Domestic Preparedness, U.S. Department of Justice. http://www.ojp.usdoj.gov/odp. *(Web site from the DOJ to help first responders deal with incidents of terrorism and weapons of mass destruction.)*
- ✔ State Offices and Agencies of Emergency Management. *(Includes state emergency manager's email address.)* http://www.fema.gov/fema/statedr.shtm

5. DEVELOP A PLAN TO COMMUNICATE INTERNALLY.

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

Examples

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

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

Resources

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

6. Develop a plan to communicate externally.

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

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

Examples

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

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

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

Resources

- ✔ "Emergency Management Guide for Business & Industry." FEMA, pgs. 41-41. *(Discusses emergency communications with the public.)* http://www.fema.gov/pdf/library/bizindst.pdf
- ✔ "The Administration of Justice Under Emergency Conditions: Lessons Following the Attack on the World Trade Center." Oren Root, Vera Institute of Justice, January 2002. *(See recommendations regarding communications on pages 25-26.)* http://www.9-11summit.org/materials 9/11/911/acrobat/26/C1TheAftermath/Vera InstituteLessonsFollowingAttack.pdf

7. DON'T LET RESOURCES PREVENT PLANNING.

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

Courts can begin with low-cost planning activities and explore opportunities for additional resources as the planning process unfolds. As courts reach out to other community and government entities to create an effective plan, they may learn of expertise that resides in the community and funding sources they do not normally access.

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

Examples

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

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

Resources

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

About the Best Practices Institute

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

The Institute was inaugurated in the fall of 2000. Its work is guided by an advisory board of chief justices, state court administrators, a court manager, a presiding judge, and a legal scholar. The intent of the Institute is to provide a central resource to which the 50 state court systems and their state trial courts can turn to obtain the field's best thinking across the spectrum of judicial administration. For more information, please visit the Institute's Web site at http://www.ncsconline.org/Projects_Initiatives/BPI/index.htm.

NCSC
National Center for State Courts

8

Chapter 1: Standard Operating Procedures

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

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

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

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

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

Topic 1: Leadership/Commitment/The Security Plan

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

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

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

Topic 2: Collaboration and Coordination

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

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

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

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

Topic 3: Self-Assessment (Audits)

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

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

Topic 4: Security Personnel (Staffing)

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

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

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

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

A. Perimeter Security

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

B. Entrance Security – Access to the Facility

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

C. Interior Security — Generally

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

D. The Courtroom

E. High-risk Proceedings and Populations

F. Administrative Offices

G. Judicial Chambers

H. Roof Exits, Hallways, and Stairwells

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

Topic 6: Incident Reporting and Recording

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

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

Topic 7: Records and Information

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

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

Topic 8: Education and Enforcement

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

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

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

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

Topic 9: Communication

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

Topic 10: Funding

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

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

References/Resources

Fautsko, Timothy F. *Courthouse Safety Training: for the Courts of Appeal of Maryland, Dept. of Emergency Preparedness and Court Security.* Denver, CO: National Center for State Courts. 2009.
< http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=151>.

New York State Unified Court System. "The Task Force on Court Security – Report to the Chief Judge and Chief Administrative Judge. October, 2005.
<http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf>.

Superior Court of California, County of San Mateo. "1999 Final Report: Courthouse Security." *Security and the Courts Resource Guide*. 1999.
<http://www.sanmateocourt.org/director.php?filename=./grandjury/1999/99courthouse.html>.

"Table of Contents." *Justice System Journal.* Vol. 28, No. 1. 2007. <http://www.ncsconline.org/D_Comm/Projects/JSJindex/JSJ_TOC/Vol28_1/vol28_1.html>.

Wisconsin Supreme Court. "SCR Chapter 70: Rules of Judicial Administration Rule 70.39." Dec 9, 2004. < http://www.wicourts.gov/sc/scrule/DisplayDocument.html?content=html&seqNo=1072>.

Chapter 2: The Self-Audit

The Nature and Purpose of a Court Security Self-Audit

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

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

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

Topics to Cover in a Security Self-Audit

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

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

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

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

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

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

How to Conduct a Security Self-Audit

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

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

Tools and Methodology for the Self-Audit

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

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

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

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

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

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

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

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

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

Evaluating the Results of a Self-Audit

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

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

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

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

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

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

Planning and Budgeting

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

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

Ongoing Management of Courthouse Security

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

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

Postscript

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

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

References/ Resources

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

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

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

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

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

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

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

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

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

Publications

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

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

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

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

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

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

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

National Sheriffs' Association (n.d.). "Physical Security Checklist, Form 1.2.1." *Trial Court Performance Standards and Measurement System.* Williamsburg, VA: National Center for State Courts. www.ncsconline.org/D_Research/tcps/Forms/Form_1 21.pdf.

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

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

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

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

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

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

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

and custody/visitation proceedings occasioned by the relocation of custodial parents.

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

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

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

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

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

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

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

Management

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

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

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

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

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

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

Prevention

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

Preparedness

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

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

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

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

A COOP plan for courts should include the following:

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

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

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

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

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

Response

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

Recovery

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

Training

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

References/Resources

American University School of Public Affairs. "Guidelines for Pandemic Emergency Preparedness Planning: A Road Map for Courts." 2007.
http://www.ojp.usdoj.gov/BJA/pandemic/Pandemic_Road_Map.pdf.

Bomb threat reporting forms are available on the Web site of the Department of Homeland Security.
http://www.dhs.gov/xlibrary/assets/ocso-bomb_threat_samepage-brochure.pdf

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

Bureau of Justice Assistance and Center for Disease Control. "A Framework for Improving Cross-Sector Coordination for Emergency Preparedness and Response – Action Steps for Public Health, Law Enforcement, the Judiciary, and Corrections." 2008.
http://www2a.cdc.gov/phlp/EmergencyPrep.asp.

Conference of Chief Judges. "Court Security Manual, State of Minnesota."
http://www.9-11summit.org/materials9-11/911/acrobat/27/P3&C10EmergencyPreparednessPlans/MinnesotaCtSecurityManual.pdf.

Conference of State Court Administrators. "Position Paper on Emergency Preparedness in the State Courts." Williamsburg, VA: National Center for State Courts. December 2006.
http://cosca.ncsc.dni.us/WhitePapers/EmergencyPreparednessStateCourts_Dec06.pdf.

COOP Planning. "Maintaining the Rule of Law – Planning for a Pandemic within an All-Hazards Context." Williamsburg, VA: National Center for State Courts and State Justice Institute.
http://riz0ep.rmxpres.com/riz0ep/viewer/?peid=38a092eb-9c0b-41b1-88eb-8e3e97dc0f55.

National Association for Court Management. "Business Continuity Management Mini Guide." 2006.

National Center for State Courts. "A Comprehensive Emergency Management Program: A Model for State and Territorial Courts." 2007.
http://www.ncsconline.org/emp/EMP%20PartI%20050307.pdf.

National Center for State Courts. "Continuity of Court Operations: Steps for COOP Planning." September, 2007.
http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=75.

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

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

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

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

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

Chapter 4: Disaster Recovery — Essential Elements of a Plan

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

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

Step One – Leadership Commitment

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

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

Step Two – Risk Assessment

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

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

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

Step Three – Disaster Recovery Plan

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

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

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

Step Four – Testing

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

Step Five – Plan Maintenance

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

References/Resources:

"Disaster Recovery Planning for Courts: A Guide to Business Continuity Planning." Williamsburg, VA: National Association for Court Management.2000. http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=0

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

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

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

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

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

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

Chapter 5: Threat Assessment

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

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

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

The Process of Threat Assessment

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

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

Identifying the Threat

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

Assessing the Threat

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

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

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

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

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

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

Investigating the Threat

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

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

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

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

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

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

Managing the Threat

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

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

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

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

Threat Assessment Training

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

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

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

Communicating with Subjects

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

Incident Tracking

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

Build Liaisons with Other Agencies

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

Conclusion

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

References

Calhoun, Frederick S. and Stephen W. Weston. "Defusing the Risk to Judicial Officials: The Contemporary Threat Management Process." Alexandria, VA: *National Sheriffs` Association*. 2001.
http://www.sheriffs.org/coda/CourtSecurityResources.asp

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

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

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

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

"Protecting Judicial Officials: Implementing Effective Threat Management Process." *Bureau of Justice Assistance Bulletin.* U.S. Department of Justice. June 2006.
http://www.ncjrs.gov/pdffiles1/bja/213930.pdf.

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

For on-line information on the evaluation tools discussed in this chapter, see
HRC http://www.violence-risk.com/hcr20annotated.pdf
Rage V: http://downloads.workplaceviolencenews.com/rage-v.pdf
SARA: http://www.violence-risk.com/risk/instruments.htm
Violence Assessment Grid: http://downloads.workplaceviolencenews.com/rage-v.pdf

Chapter 6: Incident Reporting

Importance of Incident Reporting

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

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

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

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

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

Establishing an Incident Reporting System

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Defining a Reportable Incident

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

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

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

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

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

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

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

References/Resources

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

Chapter 7: Funding for Court Security

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

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

Federal Funding for Court Security

At this time, there appears to be little in the way of direct federal funding for state courts. State and local courts have been unable to apply directly for resources. In most cases, those federal funds that are available flow from the Department of Justice or Department of Homeland Security and are dispersed to the states. On the state level, an administrative agency or official then can disperse the funds. Unfortunately, this often creates competition between the executive and judicial branches for funding.[1] There have been attempts to lobby Congress to allow state courts to apply for the federal funds directly. To date, these efforts have not been successful.

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

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

targeted to assess and enhance state court security, ensure that state and local courts are eligible to apply directly for discretionary federal funding, and ensure that state courts are included in the planning for disbursement of federal funding administered by state executive agencies.[2]

Mary McQueen, president of the National Center for State Courts, testified to a House committee on the importance of a Threat Assessment Database and a mechanism to ensure uniform collection of data and data-sharing among states. She also asked the committee to consider funding for the NICS Improvement Act, which would provide grants to state and local courts in reporting mandatory data to the National Instant Criminal Background Check System (NICS).[3] Although the House did not include the requested funding, its report accompanying the bill urged the Department of Justices' Bureau of Justice Assistance to devote resources to the problem of courthouse violence.

State Funding for Court Security

Funding for security measures in the state and local courts is generally provided by several methods: court fees and assessments, direct appropriation by the legislature, and — in some cases — donations by interested parties. Court security funding can either be under direct control of a court or the control of others.[4] These "others" who provide grants to courts may be the state supreme court or the state court administrator's office.

One issue regarding court security funding is that it is often looked upon as a budget line from which money can be taken should a state's fiscal situation worsen. In two instances below, there are efforts to take monies from the court security fund (for unspecified reasons). California has recommended creating a court security budget line item and requiring that allocations be used only for security efforts and the unused funds be allowed to roll over to the next year.[5]

[2] Bell, Robert W. *Written Testimony on Improving Security of Our State Courts*. 7 (2007).
[3] Testimony by Mary McQueen to the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies. April 2, 2009.
[4] Raftery, William. *Gavel to Gavel*. February 15, 2007.
[5] Judicial Council of California. *Recommendations on Trial Court Security Funding Standards and Methodology*. p. 3.

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

Arkansas
Arkansas has created a central fund for court security, which is distributed by the Administrative Office of the Courts.[6]

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

Colorado
Colorado created a court security cash fund commission and assesses a $5 fee on most civil actions, criminal convictions, probate filings, and traffic infractions.[7]

Note: There have been attempts to divert monies from this fund to the general fund for unspecified reasons.[8]

Delaware
Delaware imposes court assessment fees of up to $10 on civil filings and each criminal, traffic, or delinquency charge where there is a conviction or finding of delinquency or responsibility.[9] These monies are then deposited in a court security fund and maintained separately from the general fund.

Illinois
Illinois allows jurisdictions to impose a court services fee for civil actions and in convictions of criminal, local or county ordinance, traffic, and conservation cases.[10]

Maine
Maine created a courthouse security fund under Supreme Judicial Court control. It consists of all money appropriated or allocated for inclusion in the fund from whatever the source.[11]

Mississippi
Mississippi has created a state court security systems fund, and monies deposited into the fund are used by the Administrative Office of the Courts for court security.[12]

[6] For the coming year, $361,043.00 has been appropriated; 2009 Ark. ALS 1499.
[7] C.R.S. 13-1-201 (2008); C.R.S. 13-1-204 (2008).
[8] 2009 Colo. SB 208; 2009 Colo. SB 279.
[9] 10 Del. C. § 8505 (2009).
[10] 55 ILCS 5/5-1103 (2009).
[11] 4 M.R.S. § 58 (2008).
[12] Miss. Code Ann. § 37-26-9 (2008).

Montana
Montana courts apparently receive funding from the legislature. Chief Justice Mike McGrath reported that recently $300,000 was appropriated for courtrooms in Montana.[13]

Nevada
There is proposed legislation in Nevada allowing a filing fee of not more than $20 to be assessed for court security efforts.[14]

New Mexico
County commissioners are responsible for court security.[15]

Oklahoma
Oklahoma assesses a courthouse security fee of $10 for criminal actions.[16]

Oregon
Oregon's counties maintain a court security account for providing security services.[17] Courts' fees are assessed in a range of $3 - $7.[18]

Note: There has been an attempt to divert funds from the State Courts Facilities Security Account to the general fund for some unspecified reason.[19]

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

Tennessee
Tennessee assesses a $2 fee on criminal cases to be deposited into the county general fund for courtroom security.[20]

[13] 34 *Montana Lawyer* 18 (November 2008).
[14] 2009 Nev. ALS 443.
[15] N.M. Stat. Ann. § 4-41-16 (2008).
[16] 28 O.S. § 153(E).
[17] ORS § 1.182 (2007).
[18] ORS § 137.309 (2007).
[19] 2009 Ore. SB 581.
[20] Tenn. Code Ann. § 8-21-401 (2009).

Texas
Texas assesses a court fee of from $3 to $5, depending on the criminal offense, for court security purposes.[21] The county commissioners can authorize civil filing fees of from $1 to $5 ($20 in Webb County) for court security purposes.[22]

Utah
Utah has created a restricted account within the general fund known as the Court Security Account.[23] A security surcharge of $25 is assessed in all courts of record on all criminal convictions and juvenile delinquency judgments.[24] In addition to any fine, penalty, forfeiture, or other surcharge, a security surcharge of $32 shall be assessed on all convictions for offenses listed in the uniform bail schedule adopted by the Judicial Council, and moving traffic violations, of which 25 percent of that amount is to be deposited into the Court Security Account.[25] The Court Security Account also gets $15 of civil filing fees.[26]

Note: A Recent Utah House bill is trying to increase the fee amount.[27]

Virginia
Any county or city, through its governing body, may assess a sum not in excess of $10 as part of the costs in each criminal or traffic case in its district or circuit court in which the defendant is convicted of a violation of any statute or ordinance.[28]

West Virginia
West Virginia has created a special revenue fund, known as the Court Security Fund, within the Department of Military Affairs and Public Safety, which is chaired, by statute, by the supreme court administrator. The Court Security Fund may receive any gifts, grants, contributions, or other money from any source that is specifically designated for deposit in the fund.[29] West Virginia assesses $5 on each civil filing fee to be deposited in the Court Security Fund[30] and $5 on each criminal case.[31]

[21] Tex. Code Crim. Proc. art. 102.017 (2009).
[22] Tex. Gov't Code § 101.0615 (2007).
[23] Utah Code Ann. § 78A-2-602 (2008).
[24] Utah Code Ann. § 78A-2-601 (2008).
[25] Utah Code Ann. § 78A-2-601 (2008).
[26] Utah Code Ann. § 78A-2-301 (2008).
[27] 2009 Ut. HB 455.
[28] Va. Code Ann. § 53.1-120 (2009).
[29] W. Va. Code § 51-3-14 (2008).
[30] W. Va. Code § 50-3-1 (2008).
[31] W. Va. Code § 50-3-2 (2008).

For states not listed above, general court security funding is part of the general judicial appropriation by the legislature. In New York, for example, funds for court security are allocated in the proposed annual judiciary budget request.[32]

Donations by Interested Parties

In a few cases, courts have received funding from interested parties. A 1997 survey by the American Judges Association (AJA) listed bar associations as an unusual source of funding.[33] Kansas courts have received monies from the Kansas Highway Patrol to enhance physical security.[34]

Recent Attempts at Funding

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

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

References

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

[32] New York State Unified Court System. "The Task Force on Court Security: Report to the Chief Judge and Chief Administrative Judge. " p. 4 (2005).
[33] American Judges Association, *Court Security Survey Report*. 1997. Available at http://aja.ncsc.dni.us/Old%20Website/Ctsecurity.html
[34] From chart in *National Summit on Court Safety and Security Follow-Up Meeting Participant Book* (2005).

Chapter 8: Security Equipment and Costs

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

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

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

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

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

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

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

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

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

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

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

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

Duress Alarms

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

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

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

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

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

Closed-Circuit Television System

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

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

Intrusion Alarm System

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

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

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

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

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

Access Cards

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

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

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

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

Command and Control Center

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

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

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

Other Security Equipment

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

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

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

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

References

American Society for Industrial Security
<http://www.asisoline.org/>.

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

Chapter 9: Resources/Partnerships

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

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

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

Partners for Collaboration

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

U.S. Marshals Service

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

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

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

National Sheriffs' Association – Court Officers Association

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

Local Police/Sheriffs/Security Personnel

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

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

Local Government Officials

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

Local Bar Associations

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

Example of Collaboration – Department of Homeland Security

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

Positioning Courts to Facilitate Collaboration

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

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

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

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

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

References/Resources

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

Bureau of Justice Assistance and Center for Disease Control. "A Framework for Improving Cross-Sector Coordination for Emergency Preparedness and Response – Action Steps for Public Health, Law Enforcement, the Judiciary, and Corrections." July 2008.
http://www2a.cdc.gov/phlp/EmergencyPrep.asp.

Campbell, Colin F. and Marcus W. Reinkensmeyer. "The Court Security Challenge: A Judicial Leadership Perspective." *Justice System Journal*, Vol. 28, No. 1 p. 51. 2007.
http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=87.

Casey, Pamela. "A National Strategic Plan for Judicial Branch Security: Prepared for the National Center for State Courts and the National Sheriffs' Association." Williamsburg, VA: National Center for State Courts. 2006.
http://solutions.ncsconline.org/Recommended_strategies_Appendices_Final_Report_2-7-061.pdf.

Colorado State Court Administrator's Office. "Colorado Courthouse Security Resource Guide." 2008.
http://www.courts.state.co.us/userfiles/File/Administration/Financial_Services/Court_Security_Resource_Guide.pdf.

Conference of State Court Administrators. "Position Paper on Emergency Preparedness in the State Courts." p. 9. 2006.
http://cosca.ncsc.dni.us/WhitePapers/EmergencyPreparednessStateCourts_Dec06.pdf.

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

Murer, Amanda C. "Communication is the Key in Court Security in Report on Trends in the State Courts." p. 19. 2005.
http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=127.

National Center for Judicial Security. *U.S. Marshals Service.*
http://www.usmarshals.gov/oca/ncjs.htm.

National Sheriffs' Association. *Court Officers and Deputies Association.*
http://www.sheriffs.org/coda/index.asp.

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

New York State Unified Court System. "The Task Force on Court Security Report to the Chief Judge and Chief Administrative Judge." 2005.
http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf.

New York State Unified Court System. "The Task Force on Court Security: Report to the Chief Judge and Chief Administrative Judge." p. 15. 2005.
http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf.

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

Pines, Zygmont A. "Prudent Risk Management: A Court Administrator's View." *Justice System Journal*, Vol. 28, No. 1. 2007.
http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=85.

"Protecting Judicial Officials: Implementing an Effective Threat Management Process." *Bureau of Justice Assistance Bulletin*. p. 4. 2006.
http://www.ncjrs.gov/pdffiles1/bja/213930.pdf.

Chapter 10: New Courthouse Design

Importance of Security Considerations in Designing a New Courthouse

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

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

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

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

Incorporating Security into Design

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

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

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

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

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

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

Exterior Security

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

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

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

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

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

1. A strategic approach to reducing risk defines priorities; identifies correctable conditions; leverages resources to implement appropriate facility design, site design, and property management; and remains flexible to changing levels of threat.

2. A comprehensive design satisfies multifaceted site requirements to maximize functionality, aesthetics, and a total project value for its users and the community-at-large.

3. A collaborative, multidisciplinary team — including the court and tenant agencies, security professionals, designers, and community representatives — can integrate diverse expertise to create innovative and effective solutions.

4. A phased, incremental development strategy is invaluable for the successful implementation of security improvements over time, whether for a major project with multiyear execution or for multiple, small projects at one property.

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

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

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

- **Natural and constructed access control** — Natural access control focuses on limiting and providing guided access through use of properly located entrances, exits, fencing, landscaping, sidewalks and roadways, signage, and lighting. This guidance helps deter access to a crime target and creates a perception of risk to a perpetrator.

- **Territoriality** — The use of physical attributes that express ownership, such as fencing, pavement treatments, signage, and landscaping, promotes a perception that these areas are controlled. In an area that is physically designed to protect designated space, people are more likely to challenge intruders or report suspicious activity, and the design itself causes intruders to stand out.

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

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

Interior Security

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

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

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

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

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

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

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

Bibliography and Resources

Hardenberg, D. and Phillips, T.S. (eds.). "Retrospective of Courthouse Design: 1991 – 2001." Williamsburg, VA: National Center for State Courts. 2001. http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=76.

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

Judicial Conference of the United States Courts. "U.S. Courts Design Guide." Washington, DC. 5th ed. 2007. http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=113.

Judicial Council of California, Administrative Office of the Courts. "California Trial Court Facilities Standards." San Francisco, CA. 2006. http://www.courtinfo.ca.gov/programs/occm/documents/06_April_Facilities_Standards-Final-Online.pdf.

U.S. General Services Administration (GSA). "The Site Security Design Guide." Washington, D.C.: Public Buildings Service, Office of the Chief Architect. 2007. http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=23429 .

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

Utah Judicial System. "Master Plan for Capital Facilities." Salt Lake City, Utah: Administrative Office of the Courts. Vol. II. January 2008. http://www.utcourts.gov/admin/facilities/Section-II.htm.

Appendix A:

Representative Sample of Guidelines From State Court Security Manuals

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

A. Perimeter Security

1. Parking areas

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

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

2. Grounds (lighting, visibility, protective distance)

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

3. Exterior of buildings (potential access routes)

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

4. Surveillance (patrols, daily inspections)

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

5. Equipment (alarms, surveillance)

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

6. Loading docks

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

B. Entrance Security—Access to the Facility

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

☐ Access points to the facility should be limited in number, preferably limited to one main entrance (the so-called "single point of entry").

The "single point of entry" is an important component of court security because, when used in conjunction with the screening post, it greatly minimizes risk at the front end.

☐ All points of entry should be secured with adequate personnel and equipment at all times.

Limited access to a facility greatly minimizes security risks, allows better observation and detection, and helps to reduce the costs of weapons screening throughout a facility.

☐ There should be continuous monitoring of all points of entry.

2. Controlled access ("the screening post")

☐ All persons entering the facility should be screened at all times.

*Entrance screening is viewed as the single-most important element in a comprehensive courthouse security program. (For examples, see, Arizona, Ohio, Washington.) New Jersey exempts judges, and in New York, limited classes of persons – court employees, tenants of courthouse facilities, attorneys, government or non-profit agency employees who regularly conduct business within the courts – generally are not required to pass through magnetometers provided they comply with certain conditions (*e.g.*, presentation of identification cards through the court's SecurPass program, which requires a criminal background check).*

☐ There should be weapons screening at every access point.

Michigan's manual specifies that if staff and judges use non-public entrances, provisions should be made for weapons screening at such entrances. Entrances without screening should be locked and equipped with alarms and signage stating "Emergency Exit Only. Alarm Will Sound." Michigan specifies that a court's screening policy should include a list of restricted items, a secondary screening policy for people who have not successfully passed through after two tries, storage and disposal of confiscated items, protocols for appropriate responses to attempts to bring weapons in the facility, and protocols for law enforcement personnel. Michigan's manual also specifies the components of a proper weapons screening station to include adequate room for people to congregate inside, out of the weather, without being so crowded as to present additional security problems; a magnetometer, x-ray equipment, and handheld magnetometers for back-up screening; a duress alarm to summon additional help if needed; CCTV for monitoring access points; adequate staffing of at least two trained staff to monitor traffic flow and at least one officer with a weapon to observe and respond to emergencies; and access to a private area to conduct a more thorough search using same-gender personnel.

- ☐ If there is a separate entrance for judicial officers, the court's protocol should strictly prohibit admittance by any unauthorized persons.
- ☐ Items (such as purses, backpacks, briefcases, bags, boxes, laptops, CD players, cell phones, pagers, radios, etc.) should be subject to the screening process.
- ☐ Screening stations should consist of a metal detector, x-ray machine, and sufficient personnel to operate the equipment and conduct screening.

  Ohio, for example, recommends at least one portable walk-through magnetometer and one handheld magnetometer with a trained security person. The preferred security practice is to have three personnel at each security screening post: one to operate the machine, one to check persons who set off a detecting device, and a third person who can provide back-up in the event of an emergency or need for additional screening procedure. (For example, see "Gaining Access to Courthouse Security," Courts Today, *pp. 34-37, Jan-Feb 2005.)*
- ☐ There should be clearly written, visible signage at the entrance indicating the court's screening policies and list of prohibited items.

  Signage operates as a deterrent.

3. Screening of mail and deliveries

- ☐ All incoming mail and packages should be received in a central location and subjected to screening prior to delivery.

  See Wisconsin's manual (Chapter 5) for an identification of characteristics of suspicious packages and appropriate response procedures. (Also, see Washington.)

4. Personnel (at entrance points)

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

5. ID and access control procedures

- ☐ Identification procedures and protocols are helpful to reinforce entrance screening (such as card keys, identification badges, sign in/sign out, etc.). Such procedures should apply to all employees and visitors.
- ☐ Identification should be displayed at all times in the building.
- ☐ There should be strict control of all access keys and cards.

  The use of badges and card keys must be strictly controlled and monitored, especially with regard to terminated or departing employees. A log of all such ID badges and cards should be maintained. Lost or stolen cards should be reported promptly. (See Arizona SJI Project regarding monitoring and auditing access cards, and Michigan and New Jersey. New Jersey provides for electric latch or card access entry for judges' private entrances.)
- ☐ Access codes should be periodically changed (especially after a security breach) and courts should have the ability to act promptly in the event of a security breach of its identification system.

  New York, for example, utilizes a "smart card" system that physically incorporates digital chips that can be promptly deactivated. The New York security taskforce

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

6. After-hours operations

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

7. Weapons policy

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

  *The New York security taskforce recommended that all firearms carried by uniformed on-duty personnel be secured in safe and serviceable holsters with a safety rating of Level III and that all court clerks authorized to carry firearms should be required to use holsters with covered trigger guards and snap enclosures that securely attach to their belts and to wear their uniform blazers at all times. Many states prohibit law enforcement officers (when acting outside the scope of their employment) from bringing weapons into a court facility. The carrying of weapons in a court facility is a difficult practical, political, and policy issue for many jurisdictions. Some states address the issue statutorily. In a 2005 survey conducted by the Delaware Administrative Office of the Courts, the overwhelming majority of responders indicated there was no formal court policy governing whether judges are permitted to carry guns in the court facility. Some states (*e.g., *South Carolina and Kentucky) apparently permit. Rhode Island and Allegheny and Berks counties in Pennsylvania reportedly have a zero tolerance weapons policy for court facilities. (Also see Michigan, Ohio, New Jersey [which exempts judges from weapons screening], and Alabama.)*
- ☐ All personnel authorized to carry firearms in court facilities should be required to pass a qualified certification program successfully and be required to pass an annual firearms requalification program. (See Alabama.)
- ☐ There should be clear signage at the court's entrance regarding the facility's weapon policy.
- ☐ There should be secure depositories for the temporary storage of firearms.
- ☐ Unauthorized firearms and weapons should be confiscated and destroyed.
- ☐ Annual statistical reporting regarding seized weapons and contraband is advisable.

8. Other policy considerations: use of force and contraband

- ☐ Courts should have clear policies on use of force by court security personnel (when appropriate, acceptable physical responses).
- ☐ Courts should have clear policies regarding contraband items.
- ☐ Courts should have clearly stated and visible signage at court facility entrances and interiors about prohibited items subject to confiscation.

9. Custodial services

- ☐ Custodial staff should never have unsupervised access to the facility after hours.
- ☐ Custodial staff should be subject to routine security screening procedures.
- ☐ Custodial staff should be subject to initial and periodic security background checks.

  Other security protocols should be considered, such as the wearing of name/company badges, fingerprinting, specific procedures for day and night shifts, sign-in/sign-out procedures, security checks of supplies, restrictions on packages/bags, and possession of alcoholic beverages/ non-prescription drugs in the building. (See Delaware.)

10. Vendors/independent contractors

- ☐ Protocols similar to those for custodial staff should also be identified and implemented for non-employee occupants/visitors, including vendors and independent contractors working in the facility. (See Delaware.)

C. Interior Security — Generally

1. Circulation zones

- ☐ It is recommended that a court facility's space be segregated or separated into three distinct "circulation zones" – separate zones for judges and staff, the public, and prisoners.
- ☐ Access to zones should be controlled. Access keys and cards by non-security personnel should be limited and supervised by security personnel.

  *Circulation zones are mandatory in New Jersey for new or renovated court facilities. If such circulation patterns or zoning areas are not feasible, other options (*e.g.*, designating off-limits areas except for authorized personnel with I.D. cards, installation of locking devices and monitoring system) may be available. Designated off-limits areas could include HVAC/utility/computer equipment rooms or closets, chambers, elevators, work stations, unused court rooms, hallways, stairs etc. Delaware has designated security levels for areas and user groups. (Also see Arizona.)*
- ☐ Where such circulation zoning is not possible, adequate procedures should be in place to protect staff and public from prisoners (*e.g.*, by escorting prisoners with adequate security guards and using appropriate physical restraints).
- ☐ Non-authorized personnel and visitors should be restricted to public areas at all times.

2. Locking devices (utility and environmental controls)

- ☐ There should be strict control of access to all controls for the environment and utilities, which should be protected by tamper-resistant locking devices.
- ☐ There should be central administration to oversee the security of such controls.
- ☐ Outside air-intake mechanisms should be secured to prevent unauthorized access or interference. (See Michigan, Wisconsin, Arizona, and Delaware.)

3. Identification and monitoring procedures

- ☐ All personnel and authorized visitors should display appropriate identification at all times when in the facility.

  *Michigan specifies that an employee's identification card should display only the first name. New sophisticated technology is available to control and monitor access (*e.g.*, electronic access cards or biometric systems that record a person's movement in the building). For examples see New York and Michigan.*

4. Security equipment and enhancements

- ☐ Court facilities should be equipped with intrusion and duress alarms.

  Intrusion alarms are designed to alert others to unauthorized entry after hours or in restricted areas. Duress or panic alarms are designed to signal to others (usually law enforcement or security officers) the need for immediate assistance at a specific location.
- ☐ Halls, corridors, and passageways should be brightly lit and equipped with viewing mirrors.
- ☐ There should be emergency back-up for lighting.
- ☐ Ceiling panels should be secured to prevent intrusion.
- ☐ First-aid kits should be readily available throughout the facility.
- ☐ There should be properly trained personnel to operate security equipment effectively.

  *In addition to x-ray machines and magnetometers to provide entrance security, devices to provide interior security include ballistic-shielded benches; caller ID phones; card-key readers; closed-circuit television cameras (CCTV); door viewers; electronic mechanisms to control opening and locking of doors; intercoms; locks to store and secure property (*e.g.*, guns, cell phones, etc.); magnetic locks; numeric pin pads; restraining equipment (handguns, knee/ankle braces, Tasers); security lighting; and smoke detectors. Ohio recommends that, when practical, CCTV surveillance should include the court facility, parking areas, entrance(s) to court facility, courtrooms, and all other public areas of the facility.*

5. Security personnel (training and safety)

- ☐ Security personnel in the facility should be adequately trained and certified in the skills and performance standards required to fulfill their responsibilities.

  Such training should include instruction in the transportation and restraint of prisoners, facility-specific security procedures, the use of force, dealing with the public, etc. The New York court security taskforce recommends that each officer providing security to the facility should be given a copy of the facility's security protocols and acknowledge receipt thereof. (Also see New Jersey, Wisconsin [Chapter 9], Arizona [pp. 24-25], and Michigan. Arizona provides that "training of

court security personnel shall be career oriented with a core curriculum that is court security specific." New Jersey requires training in dealing with the public.

- ☐ The physical safety of security personnel to perform their responsibilities should be addressed.

  The New York security taskforce recommended a court policy that requires court officers serving in sensitive posts and patrols to wear ballistic-resistant vests approved (and perhaps funded) by the judiciary and, further, that all such vests should be standard issue for all uniformed court officers. The New York report also recommended that some (but not all) security officers should be equipped with batons and O.C. (oleoresin capsicum) pepper spray in accordance with applicable laws.

6. Internal communications (within the facility)

- ☐ Each facility should have a public address system for use in the event of an emergency (such as lockdowns, bomb threats, etc.). Evacuation routes and emergency exits should be conspicuously identified.

7. Prisoner transport/holding areas

- ☐ There should be separate and secure holding areas where prisoners can be locked up and supervised (*e.g.*, by security personnel, CCTV) while waiting to appear in court or to be returned to jail.
- ☐ Local corrections departments should notify the facility of any special category of prisoner (*e.g.*, assaulting prisoner, escape risk, suicide watch, and gang affiliation) *prior to* transport to the court facility or, at the least, upon arrival at the court facility.

  A prisoner classification system, worked out by local law enforcement and the courts, can be used to transmit critical data. For example, color-coded, high-security restraints have been successfully used to identify high-risk prisoners in their facilities quickly and easily. Also see New York security taskforce report regarding notification.
- ☐ Prisoners should have a separate circulation route away from court personnel and the public, and out of sight of jurors.

  Ohio provides that if a separate circulation route for prisoners is not feasible, then appropriate restraints (handcuffs, leg braces) should be employed. See this section for information regarding restraining devices.
- ☐ Prisoners should be monitored by cameras or tracking devices.
- ☐ Restraint equipment should be used in appropriate situations and should be readily available in the facility in the event that a prisoner becomes unruly or creates a security risk. Prisoners escorted in the courthouse should be restrained with handcuffs.

  For example, see Alabama and New York. Restraining devices include handcuffs, transport leg braces, ankle restraints, waist chains, transport/custody belts, and elastic belts equipped with stun devices. It is important to be cognizant of the dangers of prejudicing a juror who views a defendant in such restraints. The New York security taskforce recommended that a prisoner should be rear-handcuffed at all times except when appearing before a jury and during extended hearings. Holding cells could also be equipped with a small rectangular insert to provide secured access to a prisoner when handcuffs need to be removed.

- ☐ Appropriately trained and physically capable law enforcement personnel, in sufficient ratio to the perceived risk, should escort prisoners to and from the facility and courtrooms.
- ☐ There should be clear written protocols to cover the following prisoner transport issues: (1) the staffing levels required to escort prisoners, (2) the arming of security personnel, (3) physical requirements of escort personnel, (4) restraint/force procedures, (5) procedures to handle potentially volatile prisoners, and (6) emergency procedures in the event of an escape or evacuation.

  For examples, see New Jersey, Delaware, Michigan, Washington, Ohio, and Arizona. Also see the publication by the National Sheriffs' Association ("Court Security Audits, Forms, Policies, and Self-Assessment Tools") especially with regard to holding facility guidelines. A recent publication from the National Association for Court Management recommends that security personnel not carry weapons when handling detainees and that a single officer never move more than one person at a time. See National Association for Court Management, Court Security Guide, p. 21 (2005). The New York taskforce on court security, supra, *made the following recommendations regarding prisoner handling: (1) the prisoner escort court officer in control and in proximity to the prisoner should be unarmed (which is reportedly the current practice in New York City courts); (2) the number of uniformed officers transporting prisoners must be commensurate with the security risk presented* vis-à-vis *the number of prisoners being transported and the location's physical characteristics; (3) prisoners transported through public areas of a courthouse should be escorted by no fewer than two uniformed officers; and (4) courts should strictly prohibit the changing of clothes by prisoners at court facilities. Michigan's manual recommends the following standards for holding areas for temporary prisoners: holding areas should be constructed to lessen the possibility of self-inflicted injury; be inspected daily for contraband; include doors that allow for easy observation; include toilet facilities; be checked by staff every thirty minutes; have CCTV monitoring, if possible; and have a self-contained breathing apparatus.*
- ☐ Videoconferencing should be considered as an alternative to prisoner transport.

  *Videoconferencing (*e.g.*, of arraignments) entails less risk and expense. For examples, see Missouri Statutes sec. 561.031 and Pennsylvania Statutes 42 Pa.C.S., Section 8703. Videoconferencing speeds the process, minimizes risk and cost, and can be useful in a public health emergency. Such an option, however, must comport with constitutional and statutory requirements.*

8. Building/personnel profiles

- ☐ Courts should maintain confidential files regarding up-to-date personnel lists, essential personnel information (*e.g.*, contact persons, medical needs), and the facility's floor plans and allocation of space.

  This confidential information should be readily accessible in the event of an emergency or operational breakdown. Tennessee, for example, specifies that "medical and family data on each judge should be kept in the clerk's office including blood type, allergies or reactions to medication, and any other type of medical problems that should be known in case of an emergency, and the names, addresses, and telephone numbers of the next of kin."

9. Daily inspections/sweeps

- ☐ A security plan should include daily and weekly inspections of the interior as well as the exterior and adjacent areas.
- ☐ Any suspicious conditions or activities should be reported immediately and properly documented.

  See Wisconsin (pp. 27-31), Delaware, and New Hampshire (providing a helpful identification of the scope of daily security checks, which is described as "the first line approach to achieving a secure court facility"). See Arizona regarding weapons screening and daily security checklists. See section on security incident reporting.

10. Personal security: threats and risks

- ☐ There should be procedures to notify law enforcement promptly about threats against judges and personnel. All threats should be promptly documented in a security incident form.
- ☐ In preparing a comprehensive security plan, each court, in collaboration with law enforcement, should have procedures providing for the security of judges and court personnel when needed at times other than normal working hours.
- ☐ All courts should have secure parking areas for judges, staff, jurors, and witnesses who have been threatened.

  For examples, see Michigan, Ohio, Wisconsin, and New Jersey. New Jersey outlines procedures to protect members of the judiciary who receive threats. Wisconsin (pp. 79-90) identifies how to assess/rank a threat and provides information about threat assessment techniques/responses, and the U.S. Secret Service's identification of conditions that indicate a greater risk of violence. Also, see Fein and Vossekuil, "Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials," (U.S. Dept. of Justice, July 1998). See information on Element 5 (threat assessment).
- ☐ Courts should have the ability to obtain a prompt professional assessment of any reportable threat against their judges and personnel.

D. The Courtroom

- ☐ Allocation of security personnel in the courtroom should be flexible to address the risks posed in a particular proceeding, the type of case (*e.g.*, family, *pro se*, criminal), the stage of proceeding (*e.g.*, sentencing), and the extent of anticipated media coverage.

  New Jersey's recommended standard is to establish a system of allocating security personnel based upon the type of trial and the nature and number of participants involved in the given proceeding – indicators that can be classified into increasing degrees of risk (low, moderate, high). Others recommend that there should be a uniformed officer in the courtroom during all proceedings. See Arkansas, SJI Court Emergency/Disaster Preparedness Planning Project, "Planning for Emergencies," supra *at p. 11 (2005). Arizona notes that it is a recommended standard not to include in the security officer complement any officers assigned to escort in-custody participants or protected individuals.*

- ☐ If the facility does not have adequate screening at its entrances, then each courtroom should be equipped with security devices (*e.g.*, magnetometer, surveillance cameras, and duress alarms).
- ☐ The number of public entrances to a courtroom should be restricted.
- ☐ There should be a pre-determined, effective means of non-verbal communication between the court security officer and designated court personnel (*e.g.*, clerk, presiding judge) that could be confidentially used in threatening or emergency circumstances.
- ☐ There should be restricted access to light and environmental controls located in the courtroom.
- ☐ There should be a safe, quick, and accessible evacuation/egress route (via automatic locking door with peephole) in close proximity to the judge's bench.
- ☐ Coverings (*e.g.*, drapery, opaque glazing, and blinds) should be installed on courtroom doors and windows to prevent a line of sight into the courtroom.
  If feasible, windows should enhance security in terms of composition. Shatterproof windows consist of two standard sheets of glass with transparent plastic that break into a rounded grain instead of jagged shards. Bullet-resistant glass involves thicker lamination; the thicker the glass, the more resistant to the type of bullet. Bullet-resistant glass is substantially more expensive.
- ☐ Courtrooms should be locked when not in use.
- ☐ All objects (*e.g.*, furniture, flagpole, utensils) that could be used as items of assault in the courtroom should be secured or removed.
  For example, see Wisconsin (p. 51), containing an identification of "common weapons of opportunity" and recommendations for their safe use, noting that even the simplest of everyday objects can be turned into lethal weapons.
- ☐ There should be sufficient distance between the judge's bench and others (litigants, attorneys, public). The judge's bench should contain bulletproof (fiberglass resistant glazing) material and be separated by a rail from the audience.
- ☐ There should be a clear policy regarding the possession of guns in the courtroom by law enforcement and judges.
- ☐ There should be a clear policy regarding the possession of cell phones in the courtroom.
- ☐ There should be clear protocols and designated responsibility for opening, locking, and daily inspecting of courtrooms.
- ☐ Clear protocols should be in place to secure and store exhibits, especially firearms and drugs.
- ☐ Courtrooms should have essential security equipment and enhancements.
  *Important security equipment for a courtroom include silent duress/panic alarms (*e.g., *at the judge's bench, clerk's desk, sheriff's station) activated by a hidden switch/button and wired for immediate communication to a central location; ballistic shielding for judge's bench to withstand penetration of "off the shelf" bullets from handguns, including a .357 magnum; portable radios and phones (including walkie-talkie); telephone; heat/smoke detectors; CCTV, if feasible, to alert and record a security incident; intrusion alarms; emergency backup lighting and electricity; and high-quality cylinder locks on doors with a locking/release button controllable by*

judge or sheriff. (For example, see Wisconsin, Arizona, New Hampshire, Utah, Delaware, and Tennessee.)

- ☐ Court audiences should be seated at all times. Security and court personnel should be mindful of spectators attempting to change seats or move toward the bench, the parties, witnesses, or the jury. (See Alabama.)
- ☐ The number of prisoners in a courtroom at any one time should be minimized. The number of prisoners in a courtroom should be proportionate to the security provided. (See Alabama.)
- ☐ There should be clear protocols for dealing with disruptive people in the courtroom.
- ☐ In the event of a power failure where emergency power backup and ambient light are not available, there should be a continuously charging flashlight or other light source available at the judge's bench. (See Alabama.)

E. High-risk Proceedings and Populations

- ☐ As noted, it is recommended that courts establish a system of allocating security personnel based upon various factors, including the type of trial, number of participants, media coverage, and degree of risk presented.

  *Arizona notes that in assessing courtroom risk and consequent security response, a federal task force has identified the following factors as most useful in determining the need for security: whether the matter is civil, family, or criminal; the stage of the proceeding (*e.g.*, pre-trial, trial, post-trial); the type of case; the subject matter of the case; the number of persons and/or identity of other participants during proceedings (*e.g.*, witnesses, spectators); the identity of the parties to the proceedings; the extent of anticipated media coverage. Also, see Wisconsin (Chapter 4), which identifies risk levels based on the type of trial. Wisconsin notes the need for an "operational plan" that includes detailed information on protocols and procedures, specifies in advance individual and team assignments, and includes directives and essential documents, emergency response procedures, communications procedures, and command post.*
- ☐ *Pro se* and domestic litigation may require special risk assessment, security safeguards, and segregated spacing as well as clear advance communication and cooperation with law enforcement.
- ☐ Jurors should be afforded safe, secure, and separate space and should have ready access to court security officers.
- ☐ Jurors should be provided with clear, simple, written information about the court's basic security procedures as part of the juror orientation program. (See Wisconsin.)
- ☐ Special security procedures should be available for sequestered juries.
- ☐ Likewise, special security considerations should be given to victims, witnesses, and those who have received threats.

  New Jersey identified some essential considerations in drawing up a security plan for a high-risk trial as well as special considerations for civil commitment hearings at state institutions. See pp. 32-39.

F. Administrative Offices

- ☐ Administrative offices are critical to a court's operations and, therefore, should be properly protected like any other space in the court facility.
- ☐ There should be special security protocols for the handling, storage, and transport of money and negotiable instruments.

  Cash on-hand and its equivalent should be limited.
- ☐ Access to administrative offices should be controlled and monitored. Useful security measures include physical separation of staff from public (*e.g.*, by use of counters, half-walls, window shields); secure storage/locking of important files; daily inspections/sweeps of office space; controlled/supervised access by custodial or off-hours workers; locking of all doors and windows after hours; restricted access to areas housing computers, their servers, and related equipment; policy requiring the prompt reporting of suspicious packages, suspicious activity, and security breaches.

  Wisconsin (Chapter 5) provides helpful detailed advice concerning how to enhance office security generally and respond to specific situations. Arizona recommends that, when practical, there should be CCTV surveillance for the clerk's office.
- ☐ Security personnel should be readily accessible to the court's administrative offices.

G. Judicial Chambers (Controlled Access)

- ☐ Access to the chambers and staff of a judge should be strictly controlled and monitored.

  For example, see prior section on security of administrative offices. Controlled access to judicial offices can be achieved through various devices: monitors, electronic access cards, duress alarms (at desks or work stations of the secretary, receptionist, and judge), caller I.D. phones, and self-locking doors, and off-limit hallways and stairs. Ohio recommends an effective secondary screening process at the entrance to a judge's office; there should be a separate and safe work area not accessible to the public.
- ☐ All exits should be properly controlled with security devices (*e.g.*, locking devices, alarms) and monitored.
- ☐ All exits should be conspicuously identified.

Appendix B

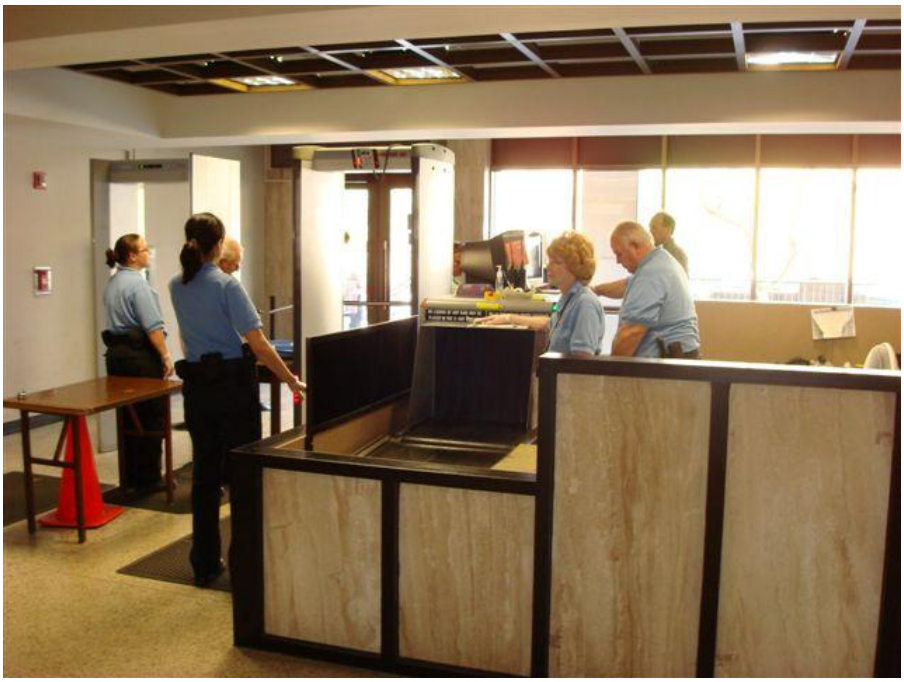
Steps to Best Practices for Court Building Security

STEPS TO BEST PRACTICES FOR COURT BUILDING SECURITY

FEBRUARY 2010

Timothy F. Fautsko
Steven V. Berson
James F. O'Neil
Kevin W. Sheehan

Daniel J. Hall, Vice President
Court Consulting Services
707 Seventeenth Street, Suite 2900
Denver, Colorado 80202-3429



Entry Screening – A Court's First Line of Defense

Acknowledgements

The development and publication of this report has been made possible by the support and hard work of many people. The National Center for State Courts (NCSC) wishes to acknowledge the four authors of this document, Timothy Fautsko, Principal Staff at the NCSC, and especially security consultants Steven Berson, James O'Neil, and Kevin Sheehan for their work in identifying the categories, topics, and steps to best practices in court security contained in this document. The NCSC also extends its appreciation to three practitioners in the field who carefully reviewed this document and made important recommendations that have improved the final product. They are Malcolm Franklin, Senior Manager, Emergency Response and Security from the Administrative Office of Courts in California; Frank Lalley, Judicial Security Administrator from the Administrative Office of Pennsylvania Courts; and Carol Price, Court Security Director from the Administrative Office of Courts in Utah. Their many years of experience in the field of court security and emergency preparedness proved invaluable in validating the many steps to best practice. Without their assistance, the quality and usefulness of information contained in this report would not have been possible. Finally, the NCSC extends thanks to its editorial staff – Ephanie Blair, Judy Amidon, and Lorie Gomez – for the many hours they spent providing quality assurance in the conformation and final editing of the report.

Introduction

The National Center for State Courts (NCSC), through its Court Consulting Division, has conducted security assessments of court buildings as well as personal security and safety training throughout the country. In conducting court building assessments, the NCSC assessment team has evaluated court security in terms of "best practices" – guidelines describing those security measures that should be in place with respect to a comprehensive set of topics covering court buildings and court operations. These best practices are not only based on the considerable experience of NCSC assessment team members, but are also a compilation of various guidelines from the U.S. Marshals Service, National Sheriffs' Association, International Association of Chiefs of Police, the Transportation Safety Administration, the Department of Homeland Security, and the National Association for Court Management. The NCSC assessment team recommends that leadership in every court building strive to achieve best practices in all topic areas to provide a suitable level of security for all those who work in or visit the court building.

Acknowledging that implementing best practices in court building security will require increasingly scarce budgetary resources, the NCSC assessment team has also developed steps in phases that can be taken toward achieving best practices in various areas of court building security. These steps may be a useful approach to courts as they strive to implement improvements in court building security. The NCSC assessment team wishes to emphasize that a fully effective integrated level of security will be reached only when all the measures at the best practices level are incorporated. The NCSC assessment team has provided these steps in phases, so that a court at its discretion can adopt incremental improvements before reaching the level of best practices. These steps in phases are plateaus along an ascending path to improvement – improvement the NCSC assessment team recommends that courts achieve over time.

It is important to note that *Steps to Best Practices* focuses almost exclusively on security matters. With rare exception, issues of emergency preparedness, continuity of operations, and disaster recovery are not within the scope of this document.

Security is not a one-time achievement. It is a serious and continuous goal and requires constant vigilance. Further, it must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and they can never be eliminated. But with proper attention and care, they can be minimized. Paying close attention to the recommendations contained in *Steps to Best Practices* will help courts minimize the risks.

Steps to Best Practices is organized by steps, phases, topics, and categories. It will be helpful for the reader at the outset to have a working understanding of each of these terms:

- Steps: These are specific buildings blocks, specific actions that courts can take to improve security.
- Phases: These are logical groupings of steps forming a temporary plateau in terms of security measures in place.
- Topics: These are the subject areas into which steps in phases are organized.
- Categories: These are sets of topics. There are four categories listed in priority order. (*Note: Topics within each category are listed in alphabetical rather than priority order.)*
    - Category A. These are fundamental topics that must be addressed first in order to provide a base on which to place all of the others.
    - Category B: These are topics that are extremely important to address.
    - Category C: These are topics that are very important to address.
    - Category D: These are topics that are important to address.

CATEGORIES AND TOPICS

Topic #	
	Category A: Fundamental
One	Command and control center
Two	Policies and procedures
Three	Security committee
	Category B: Extremely Important
One	Access of people into court building
Two	After-hours access to court building
Three	Chambers
Four	Courtrooms
Five	Court security officer (CSO) staffing levels
Six	Duress alarms
Seven	Threat and incident reporting
Eight	In-custody defendants
Nine	Training
	Category C: Very Important
One	Closed-circuit television (CCTV)
Two	Emergency equipment and procedures
Three	Interior access during business hours (circulation zones)
Four	Intrusion alarms
Five	Jurors
Six	Parking (particularly for judges)
Seven	Public counters and offices
	Category D: Important
One	Cash handling
Two	Exterior/interior patrols
Three	Perimeter issues
Four	Public lobbies, hallways, stairwells, and elevators
Five	Screening mail and packages

Category A: Fundamental

The three topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices*.

- **Command and control center**. Without such a center, the necessary and vital technological tools for court building security – closed circuit televisions (CCTV*), duress alarms, and intrusion alarms – cannot be utilized or monitored in an effective manner.

- **Policies and procedures**. Without these, there is no way to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices* to inform the process of developing a comprehensive and cohesive set of policies and procedures.

- **Security committee.** Without such a committee, meeting regularly and empowered to exercise rigorous oversight on all matters relating to security within the court building, it is difficult, if not impossible, to properly assess and address the myriad security challenges facing court leadership.

**CCTV, as used in this document, refers to a variety of old and new technologies. For detail, see topic C-1.*

TOPIC A-1: COMMAND AND CONTROL CENTER

Phase One

1. Establish a command and control center in the lobby area of the court building with an assigned court security officer (CSO*). For smaller court buildings, the monitoring function of a command and control center can take place at the front entrance screening station.
2. Provide for telephone/radio communication as a point of contact between a CSO and potentially vulnerable areas of the court building, such as courtrooms.

**Note: CSO is defined as an individual trained in court security and certified to use a firearm. The CSO should also be armed with a triple-retention holster and a radio that can communicate with the command and control center. The CSO at the command and control center does not necessarily need to be armed.*

Phase Two

Continue all steps in Phase One, plus add the following:

3. Design and construct a command and control center that is isolated from the main lobby of the court building.

4. Design a control panel that will provide space for administrative activity and equipment to monitor CCTV cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and radio dispatches.

Best Practice

Continue all steps in Phase One and Two, plus add the following:

5. Install control panels and monitoring equipment for CCTV surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch.
6. Provide additional security personnel as required to supervise and monitor command and control center activities.

TOPIC A-2: POLICIES AND PROCEDURES

Phase One

1. Judicial branch leadership understands the need for and commits to the implementation of effective, comprehensive security based on best practice models and establishes orders directing court security policies and procedures.

Phase Two

Continue with the step in Phase One, plus add the following:

2. Establish a task force under the direction of the court security committee (see Topic A-3) and with the cooperation of the appropriate law enforcement agency(s), to draft essential documents for the establishment of the policies and procedures on court building security. The task force on policies and procedures should include:
    - Court administration
    - Security personnel
    - Facilities management
    - Fire and rescue personnel
    - Others responsible for and impacted by court security
3. Create the package of essential documents to include:
    - Policies and procedures
        - Overall court security operations
        - Screening protocols
            - Define contraband that cannot be brought into the court building and confiscate it at the door.
        - Procedures to govern courtrooms and other areas in the event of a security incident
    - Risk and resource assessment instruments and protocols for use
    - Incident reporting instruments and protocols for use

- Operations manuals and materials
- Training manuals and materials
- Administrative orders with authority to revise

Phase Three

Continue all steps in Phases One and Two, plus add the following:

4. Establish communication to stakeholders that allows for feedback and adjustments as follows:
    - Assign a liaison between task force and stakeholders.
    - Provide periodic briefings in various formats to stakeholders.
    - Solicit formal feedback from stakeholders.
    - Adjust package (e.g., policies, procedures, manuals, materials) as necessary.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

5. Provide training and evaluate the package as follows:
    - Train everyone with a direct role in court security.
    - Conduct drills to test procedures.
    - Evaluate results of the drills.
    - Evaluate results of response to actual incidents.
    - Modify the package to improve practice.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

6. Review and update policies and procedures at least every other year.
7. Analyze Phases Two through Four for operational effectiveness.

TOPIC A-3: SECURITY COMMITTEE

Phase One

1. Establish a court security committee at the court building, which is chaired by a judge (preferably presiding) and has a membership of at least the primary security provider, such as the sheriff or CSO, the clerk of court, and the court administrator.
2. The judge or court administrator should meet regularly with law enforcement officials to discuss security concerns and improve security at the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Add the district attorney and public defender or representative from the state bar to the court security committee.
4. Add tenants to the security committee as appropriate.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Add elected officials to the court security committee.
6. Add an ad hoc member to the court security committee to serve on a task force for the committee.
7. Undertake a self-assessment of the security in place within the court building. Checklists with which to conduct these assessments are available from various sources, such as the National Sheriff's Association. Assistance in conducting assessments is also available from the NCSC.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Establish an integrated court security committee and use task forces to provide the committee with additional research and information gathering capacity. Additional members added to the committee or task forces should include:
    - Court staff members working in the court building
    - Local and state government officials
    - Local and state subject matter experts
9. Reconstitute the court security committee to be additionally responsible for emergency preparedness, disaster recovery/continuity of operations (COOP) plan, and response to pandemic flu, and add members with this expertise as appropriate. Rename the committee the court security and emergency preparedness committee.
10. Add planning responsibility for building new or improving current court facilities to the newly named committee.

Category B: Extremely Important

TOPIC B-1: ACCESS OF PEOPLE INTO COURT BUILDING

Phase One

1. Establish only one main door through which the public can enter the court building and display a sign at the entrance clearly listing those items that cannot be brought into the court building.
    - Designate one or more of the doors to the building to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through public entrances.
    - Keep all other exterior doors locked during business hours.
    - Emergency exit bars should be installed on all external exit doors. All exit doors should be alarmed, with ten second delay consistent with local codes. Establish signage that explains the "Exit Only" requirement.
2. Establish protocols for entry through locked doors.
    - Tailgating* or bringing in family members/friends through these doors should not be allowed.
    - Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.

    **Note: In this context, tailgating is when an individual(s) enters a court building with a person who is authorized to properly gain entry with an access card or key.*
3. Assign one CSO to guard the public entrance to the court building on a full-time basis.
4. Set up a table or other physical structure at the public entrance to serve as a screening station.
5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
    - Provide screener with a weapons ID chart.
    - Provide screener with a list of contraband items.
6. Train the CSO for all Phase One tasks described above.
7. Provide basic court security orientation training for judges and staff.

Phase Two

Continue all steps in Phase One, plus add the following:

8. Add a magnetometer at the main door (public entrance) to the court building.

9. Conduct a daily calibration and inspection of magnetometer, preferably by an authorized and trained supervisor.
10. Train CSO(s) in all tasks added in Phase Two, plus provide additional security training for judges, staff, jurors, and others.
11. Replace keys to the court building with access cards for judges, authorized court staff, and other building tenants' staff.
12. Install a CCTV camera at the main door (public entrance) to the court building.
13. Assign a second CSO* to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
14. Establish a code notification procedure between law enforcement and the court so screeners are aware if a dangerous person is likely to enter the building.
15. Add a duress alarm at the screening station.
16. Establish a policy that law enforcement officers entering the building on personal business may not bring in a weapon.

**Note: Staffing level in Phase Two is one full-time CSO at the screening station, plus one additional CSO for high-volume times.*

Phase Three

Continue all steps in Phases One and Two, plus add the following:

17. Install an x-ray machine at the public entrance screening station.
18. The second CSO referenced in step 13 should be assigned as a full-time, permanent CSO* to operate the public screening station. During slow periods, this second CSO can still be available for additional duties as described in step 13.
19. Establish additional policies and procedures for Phase Three operations as follows:
    - Conduct an annual inspection and certification of x-ray machines.
    - Provide a detailed, step-by-step manual and training on screening procedures.
20. Train CSOs in all tasks and provide security orientation training for judges and staff.
21. Add a CCTV camera at the judge/staff entrance door.

**Note: Staffing level in Phase Three is two full-time CSOs at the screening station.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

22. Assign a third CSO* to operate the public screening station: one CSO to operate the magnetometer, one to operate the x-ray machine, and one to handle problems.

During low traffic times, the third CSO can assume another assignment. Ideally, all three CSOs should be armed, but at least one should be armed. (Armed CSOs should use a triple-retention holster.)

23. If two or more public screening stations are in operation, assign a fourth CSO as a supervisor to oversee operations.
24. Install a magnetometer, x-ray machine, duress alarm, and CCTV camera to the judge/staff entrance. Consider allowing jurors to use this entrance.
25. Assign at least two CSOs to the judge/staff entrance if staff or jurors use this entrance and at peak hours during the day. Otherwise, assign at least one CSO.
26. Establish a universal screening policy. Universal screening means everyone entering the building is screened.
27. When everything is in place, establish a policy that only law enforcement officers with responsibility for court security inside the building may bring a weapon into the building. Other law enforcement officers should be required to check their weapons in a lock box at the screening station(s).

**Note: Staffing level in Best Practice is three full-time CSOs for each public screening station, plus one additional CSO to supervise multiple stations, and two CSOs assigned to judge/staff/juror entrance.*

TOPIC B-2: AFTER-HOURS ACCESS TO COURT BUILDING

Phase One

1. Permit access into all areas of the court building via key or electronic card access. Keys and cards should be issued and controlled pursuant to a comprehensive accountability system that has been approved by the court's security committee.
2. Conduct background checks prior to issuing a key or access card to any person.
3. Conduct background checks for cleaning crews and any vendors granted after-hours access to the building. Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court.
4. Monitor the activities of the public while in the building after hours.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Eliminate the use of keys and implement the use of an access card system. As necessary, issue keys to a limited number of people only for emergencies, building maintenance purposes, and building security responsibilities.
6. Create a single access point into the court building that is guarded by a CSO who checks IDs and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
7. Update background checks periodically (at least annually).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

8. Conduct a full screening requiring everyone to go through the magnetometer and x-ray station.

TOPIC B-3: CHAMBERS

Phase One

1. Install a duress alarm at the judge's desk and in the chamber's reception area.
2. Test duress alarms regularly – at least monthly.
3. Provide training to judges regarding personal security and safety in chambers.
4. Escort judges when leaving a chambers area for a courtroom if chambers hall is unsecured.
5. Keep existing chambers window coverings adjusted so activities cannot be observed from outside the court building.
6. Conduct daily sweeps of chambers in the morning and at the end of the day.
7. Keep entrance doors to chambers area locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Assign at least one CSO or transport deputy to be present whenever an in-custody defendant is escorted through chambers hallway.

Phase Two

Continue all steps in Phase One, plus add the following:

9. Install vertical blinds as interior window coverings in all chambers.
10. Install duress alarms in conference room(s).
11. Plan for and conduct drills regarding emergency situations in chambers area.
12. Escort judges when leaving secure chambers and courtroom area.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

13. Assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallway, with one to clear the path ahead. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
14. Install ballistic-resistant material in all accessible windows (e.g., ground level, first floor). The recommended ballistic-resistant material should meet UL Standard 752, Level IV, unless a lower level can be justified by an assessment of the risks

based on such factors as adjacent structures and geographic features associated with the location of chambers. This level may be reduced based on specific security assessments.

15. Request cleaning crews to clean chambers at the end of the day when court staff is present, rather than at night.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

16. Install CCTV cameras in chambers hallways that lead to the entrance to chambers areas.
17. If feasible given the existing structure of the court building, establish a secure path for judges to go from chambers to courtroom (no escorting of in-custody defendants). If feasible, establish a secure path to escort in-custody defendants from holding cells to the courtroom without going through chambers hallways.
18. Install ballistic-resistant material in all chambers windows that are located on floors above ground level.
19. Prohibit cleaning crews from entering chambers unsupervised at any time. Require cleaning during the day or leave waste baskets outside locked chambers area doors at night. The judge or court staff should be present when cleaning crews are physically cleaning/dusting chambers during the day.

TOPIC B-4: COURTROOMS

Phase One

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a "rover" from one courtroom to the next (unless local or state rules require additional coverage). There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.
2. Install duress alarms in the courtroom at accessible locations:
    - On top of or under the working surface of the bench, plainly marked
    - At the CSO station
    - At the clerk's station

    Train judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high-visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)

5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.
6. Install and then regularly test emergency lighting/fire equipment in courtrooms.
7. Always keep front and back doors to courtrooms locked when courtroom is not in use.
8. Use proper and acceptable restraints per state law on in-custody defendants.
9. Prohibit use of camera/cell phones in the courtroom and prohibit other items that could be used as weapons.

Phase Two

Continue all steps in Phase One, plus add the following:

10. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in the courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present.
11. Install one CCTV camera in criminal and family courtrooms.
    - The camera should be installed in the back of the courtroom in order to monitor activities in the courtroom up to and including the well and bench area.
12. Holding cells in the courtroom should be properly constructed and escape-proof.
13. Every three or four months, debrief incidents that have occurred in the courtrooms and review procedures related to courtroom security. This debriefing should take place in the courtroom. There should be an immediate debriefing on any serious security incident.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

14. A second CSO should be assigned to a courtroom whenever any court proceeding is being held. Whether or not there is an in-custody defendant, one CSO should be assigned for the judge and one for the courtroom. A second CSO is not ordinarily needed for civil cases, unless specifically requested by a judge based on a determination of a higher risk involved in a particular case.
15. Install one CCTV camera in all remaining courtrooms.
    - The camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
16. Install two CCTV cameras in criminal and family courtrooms.
    - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
    - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.
17. Begin the process necessary to establish a courtroom in the jail for

advisements/arraignments and other hearings. Use video arraignment* originating from the jail for in-custody hearings as much as permitted by state law.

**Note: Video arraignment is the preferred solution to bringing in-custody defendants back and forth for settings and brief hearings.*

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

18. For high-visibility trials, an additional CSO should be assigned to be present in the courtroom.
19. Use video or a courtroom in the detention center for all arraignments or hearings to set dates of next appearance.*

**Note: Use of video is the preferred solution to personal appearance by in-custody defendants whenever legally feasible by state law.*

20. Conduct sweeps of all courtrooms, including the random use of trained dogs.
21. Provide separate working offices (not in the courtroom) for clerks and others to use after courtroom proceedings have been completed.
22. Use bullet-resistant materials when constructing or retrofitting the bench and workstations inside the courtroom. The most recent recommended standard for these materials is UL Standard 752 Level III.
23. Install two CCTV cameras in all courtrooms.
    - One camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
    - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom.

TOPIC B-5: COURT SECURITY OFFICER (CSO) STAFFING LEVELS

Phase One

1. One CSO* should be permanently assigned to the main entrance of the court building during business hours.
2. One CSO or transport deputy should be assigned to the courtroom while there is an in-custody defendant in the courtroom.
3. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a rover from one courtroom to the next. There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.

**Note: It is estimated that each CSO post requires approximately 1.33 full-time employees to cover for sick leave and annual vacation, training, etc.*

Phase Two

Continue all steps in Phase One, plus add the following:

4. As additional CSOs become available, assign in the following priority per recommended phases leading up to Best Practices in each relevant topic:

    - To meet recommended staffing guidelines at screening station (see Topic B-1)
    - To meet recommended staffing guidelines for the courtroom (see Topic B-4)
    - To meet recommended ratios for transporting in-custody defendants (see Topic B-8)
    - To assign patrols for the interior and exterior of the building (see Topic D-2)

Best Practice

Continue all steps in Phases One and Two, plus add the following:

5. Achieve full recommended staffing guidelines for the following topics:
    - Screening stations (see Topic B-1)
    - Courtrooms (see Topic B-4)
    - Transporting in-custody defendants (see Topic B-8)
    - Regular patrols of building interior and exterior (see Topic D-2)

TOPIC B-6: DURESS ALARMS

Phase One

1. Install duress alarms in the courtroom and at the bench, clerk's station, and CSO station. Training should be provided on the functionality of duress alarms and on the protocols for use.

Phase Two

Continue step in Phase One, plus add the following:

2. Install alarms in each chamber and reception area.
3. Install alarms at public counters, cash areas, and other offices where the public has access, including those without counters.
4. Install alarms in the interview and mediation rooms.
5. Install alarms and 911 contact ability at the childcare center, if the court building includes such a center.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. Install alarms at screening stations.
7. Install an alarm in the jury assembly room.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install duress alarms in the holding cell area.
9. Install a duress alarm in the loading dock area.
10. Install a duress alarm in the mailroom.

TOPIC B-7: THREAT AND INCIDENT REPORTING

Phase One

1. Establish a policy requiring incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible. The more serious the incident, the more quickly it should be reported.
2. Train CSOs and staff in the court building on how to define what an incident is and how to report incidents verbally and in writing.
3. Develop and use an incident reporting form and submit forms in writing to the proper authorities, at least on a monthly basis.

Best Practice

Continue all steps in Phase One, plus add the following:

4. Implement a practice for periodically evaluating incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court security committee (and the committee's incident reporting task force).
5. Provide general feedback to staff on incidents, particularly to those who reported them (e.g., complete the feedback loop).

TOPIC B-8: IN-CUSTODY DEFENDANTS

Phase One

1. Assign at least one CSO or transport deputy to escort in-custody defendant(s) through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO or transport deputy to remain with defendant(s) in the courtroom

at all times.

3. Efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum.
4. When transporting in-custody defendant(s) in public hallways, bystanders should be moved to one side of the hall. When transporting in-custody defendant(s) in a public elevator, the elevator should be cleared of all other people.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the prisoner should be unarmed; the other officer should be armed.
6. Make sure all holding cells and areas within the court building are appropriately structured, secured, staffed, and searched daily.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Install CCTV cameras along entire in-custody defendants' escort route.
8. Establish a secure sally port for in-custody defendants entering the building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

9. Establish a secure pathway for a defendant from the transport bus, through the sally port, to the holding cell and the courtroom to avoid crossing the path of judges, staff, or public.

TOPIC B-9: TRAINING

Phase One

1. CSOs should be trained in court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, and safety and weapons certification.
2. New judges and court staff should receive an initial court security orientation briefing that includes emergency procedures, building evacuation routes, building emergency color code system, and personal safety procedures for work and home.
3. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.

Phase Two

Continue all steps in Phase One, plus add the following:

4. All CSOs should receive at least 16 hours of mandatory in-service training on court security each year.
5. Establish a judge and staff security education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and at home.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

6. In addition to annual qualification with firearms, establish mandatory refresher court security training programs for CSOs, to include such topics as emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage, shooter-in-place, and judicial protection.
7. Establish mandatory, ongoing security and safety education programs for judges and court staff that include such topics as handling difficult people, home safety techniques, safety practices for inside and outside the court building, hostage incidents, and emergency evacuation from the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

8. In addition to annual qualification with firearms, establish annual mandatory refresher court security training programs for CSOs to include first-aid, defensive tactics, handcuffing, courtroom security, and judicial protection.
9. Establish mandatory ongoing security and safety education programs for judges and court staff that include handling difficult people, high-profile trials, home safety techniques, safety practices inside and outside the court building, hostage incidents, travel safety tips, threats, and emergency evacuation from the court building.
10. Train judges and court staff in self-defense and techniques for hostage-taking situations.

Category C: Very Important

TOPIC C-1: Closed Circuit Television (CCTV)

Phase One

1. Install a digital and color CCTV camera system* at the entry screening station and in the courtroom(s) facing the gallery.

**Note: CCTV systems can utilize various kinds of technology to transmit video images and to provide for system access and control. Cables have been the traditional means of system connectivity. Newer technologies have emerged over time. Some systems now utilize an internet protocol (IP) to transmit data and control signals over a fast Ethernet link. Another technology, virtual local area network (VLAN), allows authorized personnel to access cameras or a recorder from a remote setting. Courts are encouraged to explore and adopt the technologies that best suit their needs and budgets.*

CCTV cameras should have the following functional capacity:

- Fixed or pan, tilt, zoom. These types of CCTV cameras are typically used by most courts. Fixed cameras with a wide-angle lens allow for a stationary focus on areas of interest. The capacity to tilt and pan allows each camera to maximize its area of coverage, thereby minimizing blind spots and the number of cameras needed. The ability to zoom allows each camera to capture a more accurate and close-up picture of what is actually transpiring in a particular scene.
- Color. This is standard in current systems. Black-and-white images cannot tell the full story. Important features are indistinguishable. Only with a color monitor can faces and other specific objects be clearly identified.
- Recording capacity. The CCTV system should have digital video recording capacity enabling a CSO to view incidences at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation issues. The operation and recording function of a camera can be set to activate by either motion or sound, or by the setting off of duress or intrusion alarms.
- Signs. Notices should be conspicuously placed to inform the public that CCTV cameras are operating and recording activity in the area.

Phase Two

Continue the step in Phase One, plus add the following:

2. Install CCTV cameras in detention areas to monitor activities in holding cells.
3. Install CCTV cameras on building perimeters and in secure parking lots.

4. Install CCTV cameras to monitor activity at public counters and in offices where the public may visit.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Install CCTV cameras at the loading dock.
6. Install CCTV cameras in hallways.
7. Install CCTV cameras in each courtroom.

Phase Four

Continue all steps in Phases One, Two, and Three, plus add the following:

8. Install CCTV cameras in elevators and stairwells.
9. Install CCTV cameras at screening stations.

Best Practice

Continue all steps in Phases One, Two, Three, and Four, plus add the following:

10. Install CCTV cameras in hallways that access chambers.
11. Install CCTV cameras in the mailroom.
12. Install CCTV cameras in the childcare area, if such an area exists.
13. Install CCTV cameras to cover all pathways through which an in-custody defendant may be escorted.
14. Install CCTV cameras to cover the interior areas of all doors to the court building and all accessible windows.

TOPIC: C-2 EMERGENCY EQUIPMENT AND PROCEDURES

Phase One

1. Use emergency color codes to designate emergency procedures for evacuation. An example of such a code system is attached as part of the Appendix.
2. Have an emergency, battery-generated lighting system in courtrooms, offices, and public areas.
3. Have a fire extinguisher on each floor, with egress floor plans posted.
4. Have fire alarms placed on each floor.
5. Have an elevator(s) that meets state and local fire codes, i.e., the national fire code that was developed after the MGM Grand Hotel, Las Vegas, Nevada fire, November 21, 1980.

Phase Two

Continue all steps in Phase One, plus add the following:

6. Have an emergency generator system that is properly fenced-in and protected.
7. Test generator system monthly; keep a log of tests.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Have CCTV cameras installed in the elevator(s).
9. Have automated external defibrillators (AEDs) located accessibly on each floor and designate a person(s) in the court building who is trained to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
10. Designate a floor warden on each floor to ensure proper response to emergency codes.
11. Have an enunciator fire alarm and extinguisher system.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

12. Have a floor warden identified and trained on each floor to respond to medical emergencies (e.g., CPR and use of the AED) as 911 is called.
13. Designate a safe area for a command and control center during an emergency.
14. Consider advising judges and staff by public address system, bull horn, email, or phone. One method of warning is the use of Court Building Warning Codes; a sample can be found in the Appendix.
15. Have an evacuation plan that everyone in the court building has been familiarized with.
16. Have a bomb-threat protocol and a lockdown plan in place.

TOPIC C-3: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES)

Phase One

1. Establish the concept of circulation zones (separate areas and routes) for the following:
    - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, back of public counters, private elevators, secure stairways)

- In-custody defendant transport (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms)
- Public (e.g., restrict the public to public zones)

2. All doors that are required to be locked, in accordance with the court buildings circulation zone concept, should be kept locked at all times. Such doors should never be left propped open.
3. Have a key or access card system to control access based on a system approved by the administrative authority of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience. This system should
   - Be under the control of a central authority
   - Require background checks for all card or key holders
   - Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination)

Phase Two

Continue all steps in Phase One, plus add the following:

4. Eliminate keys and require access cards. Maintenance staff and emergency responders should retain keys.
5. Establish viewing ports (peepholes) to help prevent non-authorized access through secured courtroom doors.
6. Improve definition and enforcement of circulation zones.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

7. Establish some form of video recognition (phone) system to allow access into secure areas.
8. Continue to improve definition and enforcement of circulation zones.
9. Install a CCTV camera system in all secure areas in the court building to monitor activity.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Establish and maintain maximum separation among zones (e.g., in-custody defendants are not escorted through secure hallways; judges do not pass through public areas when going to and from their cars, through screening, and to and from chamber areas.)

TOPIC C-4: INTRUSION ALARMS

Phase One

1. All exterior doors should have basic intrusion alarm devices, covering
    - All locked doors after hours
    - Emergency exit doors during business hours

Phase Two

Continue the step in Phase One, plus add the following:

2. Install intrusion devices on all accessible windows, either glass-break or motion detector.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

3. Establish a fully integrated intrusion system with the following functionalities:
    - When a court building is closed, every external door should be equipped with a device that will trigger an alarm at the control center of the appropriate responding agency and identify the intruded area.
    - During business hours, every door that is kept locked should be equipped with a device that will trigger an alarm that will identify the area intruded at the command and control center within the building. Every locked door with an emergency exit bar should trigger an alarm whenever anyone uses it, with a ten-second delay consistent with local codes
    - When the building is closed, this alarm should go to the control center of the appropriate responding law enforcement agency; when the building is open, the alarm should go to the building's command and control center.
    - All windows that are reasonably accessible from the exterior perimeter of the building (e.g., first floor, basement, possibly second floor) should be protected against intrusion. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

4. Integrate CCTV cameras into the system described above so that cameras will be activated in the area(s) of intrusion.

TOPIC C-5: JURORS

Phase One

1. Provide jurors with court security information before they report for duty by placing information on the jury summons they receive. For example:
    - Where to enter the court building
    - What items (e.g., knives, nail files, scissors) should not be brought into the court building
    - Not to discuss cases with anyone before and during jury service
    - Not to wear juror ID badges outside the court building
2. Screen jurors as they enter the court building or before they report to the jury assembly area.
3. Give a basic security and building evacuation orientation and ID badge to jurors at the assembly area before going to the courtroom. Cover such matters as what to do in case of an emergency and how to respond to a coded emergency announcement.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Assign a CSO to the jury room whenever juror payment is being made and when juror funds are obtained and transported back and forth to the court building.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

5. Assign a CSO to provide security inside and outside the jury assembly room when jurors are present.
6. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervise the loading of jurors and another CSO should meet the jurors on the floor on which they disembark.
7. Assign a CSO to remain with the jury during the entire trial/deliberation.

TOPIC C-6: PARKING (PARTICULARLY FOR JUDGES)

Phase One

1. Remove all signs in judges' parking area that identify spots either by name or title of judge. Any signs should simply say reserved along with a number as appropriate.
2. Each judge should notify law enforcement officials or a CSO of their arrival in the morning and be escorted into the court building if they park in an unprotected public parking lot.
3. Judges should be escorted to the unprotected parking lot by a CSO when they leave at night.

Phase Two

Continue the steps in Phase One, plus add the following:

4. Fence in the judges' parking lot and require that an electronic card access system is used for entrance into the court building. Install privacy slats if a chain-link fence is used.
5. Judges and court staff should be escorted to their cars or other mode of transportation after business hours.

Phase Three

Continue the steps in Phases One and Two, plus add the following:

6. Provide secure parking for judges, court staff, and jurors.
7. Install CCTV cameras in secure parking lots.
8. Provide judges and court staff a regular patrol presence in the parking areas in the morning, during the lunch hour, and at close of business.

Best Practice

Continue the steps in Phases One, Two, and Three, plus add the following:

9. Provide a secure parking area, preferably covered, for judges where they can proceed directly from their car, through screening, to their chambers without traversing any public areas or main court building entrance areas.

TOPIC C-7: PUBLIC COUNTERS AND OFFICES

Phase One

1. Install one or more duress alarms at the main public counter. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in offices (e.g., drapes, blinds) lowered to restrict observation from outside.
3. Install Plexiglas-type enclosures at cash counters.
4. Keep cash and checks in a secure, locked area overnight.

Phase Two

Continue all steps in Phase One, plus add the following:

5. Install Plexiglas-type enclosures at all public counters.
6. Install duress alarms strategically in the back areas of offices.
7. Keep cash and checks and daily change locked in a safe overnight.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

8. Install CCTV cameras at all public counters.
9. Install an alarm on the safe.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

10. Install CCTV cameras overlooking the safe.
11. Provide regular security patrols by CSOs at the public counters.

Category D: Important

TOPIC D-1: CASH HANDLING

Phase One

1. Develop and train court staff on procedures for handling cash. The procedures should:
    - Determine who should collect the money
    - Determine how to safeguard money during the daytime work hours and overnight
    - Train staff on how to verify checks and reconcile fees
    - Determine industry standards for deposits
2. Install protective barriers and duress alarms at cash counters.
3. Use an office safe for money storage.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Install CCTV cameras at counters and in the office.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Use an armored car service or the bank's personnel to pick up funds daily.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require two people – one court staff and an armed CSO – when carrying cash.

TOPIC D-2: EXTERIOR/INTERIOR PATROLS

Phase One

1. Request that the local law enforcement agency conduct exterior patrols, particularly during times when the building is closed.
2. Develop a memorandum of understanding (MOU) with local law enforcement regarding which agency is responsible to protect the exterior of the court building during and after business hours.

Phase Two

Continue all steps in Phase One, plus add the following:

3. Conduct regular CSO interior patrols by CSOs assigned to work in the court building, focusing on crowded hallways.
4. Assign CSO exterior patrols both regularly and randomly throughout the day.

Phase Three

Continue all steps in Phases One and Two, plus add the following:

5. Continue to increase both interior and exterior CSO patrols of the court building.

Best Practice

Continue all steps in Phases One, Two, and Three, plus add the following:

6. Require scheduled patrols of all interior and exterior areas 24/7, either by CSOs or local law enforcement officers.

TOPIC D-3: PERIMETER ISSUES

Phase One

1. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness. It should also be sufficient for perimeter CCTV cameras to capture images.
2. Keep doors locked after hours and allow access only via appropriately authorized key or access cards.
3. Keep all shrubbery and trees properly trimmed to prevent hiding places or access to the court building roof for persons or packages.
4. Conduct daily security checks around the perimeter.

Phase Two

Continue steps in Phase One, plus add the following:

5. Provide a secure parking area for judges with signs that do not indicate that the space is being used by a judge (e.g., signs should not say for official use only).
6. Install intrusion alarms to cover all exterior doors and accessible windows.

Phase Three

Continue steps in Phases One and Two, plus add the following:

7. Install CCTV cameras around the perimeter (at each corner of the court building).
8. Install bollards as necessary outside selected (main) entrance doors, ground floor (accessible) windows, and other vulnerable areas.
9. Enclose and secure all exposed utilities.

Best Practice

Continue steps in Phases One, Two, and Three, plus add the following:

10. Replace keys with an electronic card access system (except for back-up emergency) on exterior door entrances to the court building.
11. Provide secure parking for staff and jurors. Secure parking for judges and staff should have the following attributes:
    - Protected from public access
    - Protected from public view
    - Required electronic access, by way of card or other appropriate device
    - CCTV cameras in place and operating

TOPIC D-4: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

Phase One

1. Provide emergency lighting in the court building.
2. Establish egress/ingress standards regarding stairwells, hallways, and elevators.
3. Establish emergency procedure and evacuation diagrams.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Designate secure and public elevators.
    - Provide secure elevator(s) for judges.
    - Provide secure elevator for prisoner transport.
5. Install appropriate signage to alert the public to what items cannot be brought into the court building (i.e., guns, knives, scissors).

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Install CCTV cameras in lobbies, hallways, stairwells, and elevators in the court building and provide secure elevator(s) with electronic card access.
7. Assign a CSO to regularly patrol these areas in accordance with an assigned schedule.
8. Install a public address system in the building to facilitate announcements and emergency codes.

TOPIC D-5: SCREENING MAIL AND PACKAGES

Phase One

1. Provide routine visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items.
2. Require staff to attend training on postal security and package identification techniques provided by the United States Postal Service (USPS).
3. Develop and practice a response protocol with law enforcement when a package is identified as suspicious or dangerous.

Phase Two

Continue all steps in Phase One, plus add the following:

4. Require all mail and packages to be processed through an x-ray machine.
5. Require everyone delivering mail or packages to pass through the magnetometer.

Best Practice

Continue all steps in Phases One and Two, plus add the following:

6. Best practice is to establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:

    - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious) upon being received at the mailroom. This includes USPS mail delivered/ picked up by court staff from the local post office.

- Deliveries of flowers, candy, food, gifts, etc., to any person located in a court building should be cleared through the mailroom first, be verified and vouched for by the recipient, screened as appropriate, and then delivered.
- Mailroom staff should sort incoming mail and packages off site by building, division, and/or department and prepare them for acceptance by designated representatives of each court office or division.
- Designated representatives of each court office or division should go to the mailroom, pick up mail for distribution to their offices, and identify questionable items. All authorized court and other staff mail handlers should attend training on handling suspicious mail. Local USPS or postal inspectors may conduct advanced training for state and local government agencies.

Sample Court Building Color Codes

Professional emergency responders advise that, as much as possible, communication during an emergency should be clear, understandable, and simple. Presently, state and local courts use different warning systems and language to advise court building occupants what to do during an emergency. The decision whether to stay or leave a court building during an emergency often can be the difference between life and death.

Realizing that clear communication and understandable instructions are vital, courts have been advised by the NCSC to use universal color codes and practice drills to augment their existing evacuation procedures. Using the same color-coded language in every court building will ensure that employees will understand and react properly to emergencies.

- **Code Yellow – Situational Awareness**
  - Cautionary: Be aware and prepared to react to danger.
  - A dangerous situation may be developing in the court building.

- **Code Red – Imminent Danger**
  - Stay put! An active shooter is in the court building or there is a hostage situation.
  - Get into an emergency protective posture or in a safe haven.

- **Code Green – Emergency – Evacuate Building**
  - Listen to instructions from your floor warden.
  - Report to your assigned location away from court building.

- **Code Blue – Emergency Team Responding**
  - An emergency team is responding to or is in the court building.
  - Wait for further instructions from officials.

- Code White – **Administrative/Informational**
  - Return to normal operations.
  - All is well.

Appendix C

Home Security Audit and Recommendations

National Center for State Courts

HOME SECURITY AUDIT AND RECOMMENDATIONS

Even though reports indicate that judges and other judicial branch personnel are more likely to be injured in a fall at home or in an automobile accident than in a work-related assault, increased violence in recent years has resulted in three judges being murdered at home. These deaths were directly connected to cases over which they presided. The home security audit that follows is designed to identify security risks and provide judges and other judicial branch personnel with basic personal security recommendations that can be used to protect them and their homes.

PERIMETERS/EXTERIOR OF THE HOME

1. Does the home have perimeter lighting? Yes ☐ No ☐

   Recommendation: It is important that the entire yard is illuminated at night, without shadows.

   Recommendation: Install motion detector lights for interior and exterior protection. Outside motion detector lights can be installed to automatically turn on interior lights, giving the impression someone has entered a room, at the same time the outside lights turn on.

2. Does the home have trees and shrubs that are overgrown to the point where they block easy view from within? Yes ☐ No ☐

   Recommendation: Trim or remove thick shrubbery from window areas and replace them with shrubs that have thorns, like roses, near windows.

   Recommendation: Trim or remove trees that may provide access to upper floor windows or balconies, and make sure trees or shrubs do not block a clear view of entries and windows from the street.

3. Does the home have outbuildings (detached garage, pool house, storage buildings) located on the property? Yes ☐ No ☐

   Recommendation: Include all outbuildings into the main security system. Install quality residential locks on the buildings.

4. Do all perimeter doors provide protection from intruders? Yes ☐ No ☐

   Recommendation: All perimeter doors should be solid core wood or steel with a deadbolt lock, in addition to any other locking device.

   The door should have a peep hole installed to view any visitors prior to granting access to the home. No glass should be on the door that can be broken to gain entry. It is important that a three-inch strike plate for screws be installed in all entry doors.

   Recommendation: Secure sliding glass doors with pins to prevent both horizontal and vertical movement, especially when the home is left vacant for an extended period of time. Sliding glass doors should be hung so that the sliding door is mounted on the inside. The door should be reinforced with a "jimmy-proof" bar to prevent forced entry.

   Recommendation: Re-key or replace locks if keys are lost or stolen or if you move into a previously occupied residence. Make sure that you follow strict key control with keys used to access the home.

   Recommendation: Be sure to restrict the number of keys to your residence. Keep keys in your possession. Do not hide keys outside under the mat, over doors, in mail slots, or in potted plants.

5. Are basement windows to the home secured? Yes ☐ No ☐

   Recommendation: All basement windows should be secured from inside the home. Glass basement windows should be replaced by polycarbonate material or reinforced with decorative security bars. All ground shrubs in proximity to the basement windows should be trimmed or removed so that they do not provide potential intruders with cover from observation.

6. Does the home have an attached garage? Yes ☐ No ☐

   Recommendation: Whenever possible, park vehicles in the garage. Always enter the vehicle from inside the garage. Always keep the garage doors closed and locked when not in use. In order to limit your exposure outside the vehicle during the hours of darkness, install an automatic garage door opener and make sure all family members know how to operate the garage door

manually in the event of an emergency. Ensure that the door from the garage into the main house itself is a solid core door with a deadbolt locking device.

Recommendation: If there is a vehicle parked outside, make sure the area is well-lighted. If at all possible, have a remote starter installed in all vehicles, especially if they are parked outside. This device will allow you to start your vehicle from a safe distance.

7. Does the mail box or the entry of the home personally identify the occupants? Yes ☐ No ☐

Recommendation: Remove any identifying information from the mail box or entry of the home.

INTERIOR OF THE HOME

1. Does the home have an anti-intrusion alarm system? Yes ☐ No ☐

Recommendation: Consider installing an anti-intrusion alarm system in the home that is tied into the local police department or a certified central alarm monitoring organization. Instruct family members on the operation of the system. Consider installing a local enunciation system or siren. The advantage of a siren is to alert neighbors to notify authorities, should the direct-connect alarm lines be compromised.

Recommendation: As an added security measure, alarm systems can be customized to provide monitoring for fire, medical alert, and closed circuit television (CCTV) surveillance of home exterior. The presence of cameras on the outside of the home is a definite deterrent to would-be intruders.

Recommendation: If you have a monitored intrusion detection system, display the monitoring company's decal or sign prominently on doors, windows, and in the yard to announce the presence of a security alarm system in the home.

2. Do you have smoke/heat detectors installed throughout the home? Yes ☐ No ☐

Recommendation: Smoke alarms and heat detectors should be installed throughout the home. They should be hard-wired into the home's electrical system with a battery backup in the event

of a power failure. In addition, install and maintain all-purpose fire extinguishers throughout the home, especially in the kitchen.

Recommendation: Establish and periodically test fire evacuation procedures for all family members.

3. Is the exterior door leading from the basement to the upper floor made of solid core and equipped with a deadbolt lock? Yes ☐ No ☐

   Recommendation: As with other exterior doors in the home, it is important that the basement door be of solid core wood or steel construction and equipped with a quality deadbolt lock to prevent entry by intruders.

4. Can the interior of the home be accessed through windows or other openings from the second floor or roof? Yes ☐ No ☐

   Recommendation: All second floor windows and roof skylights must be secured to prevent access by intruders who could use drainpipes and other means to access the roof or upper floors.

5. Does the home have louver-type windows? Yes ☐ No ☐

   Recommendation: Louver windows should be replaced with solid windows made with tempered or shatterproof material.

6. Do all windows have adequate window coverings? Yes ☐ No ☐

   Recommendation: Windows should be equipped with internal blinds, curtains, drapes, or shutters to prevent someone from seeing inside.

CONDOMINIUM AND APARTMENT SECURITY

Security in condominium and apartment complexes must be a cooperative effort between residents, management, maintenance workers, and police. All must work together to provide the best possible security for the building. Most of the recommendations for single-family dwellings apply to condominiums and apartment complexes. The following is an audit that is particular to those type buildings.

1. Do all doors and windows have locks that will secure the condominium/apartment while it is vacant? Yes ☐ No ☐

   Recommendation: Examine all locks on doors and windows to ensure they are working properly. Before leaving the

condominium/apartment, make sure all doors and windows are locked. Always double-check locked access windows that are at ground level.

2. Does your complex have a separate "Laundromat" area? Yes ☐ No ☐

   Recommendation: If at all possible, avoid using the Laundromat in your complex by yourself. Always team up with a neighbor who you know and trust.

3. Does your complex have a building association or a way to alert residents of an emergency? Yes ☐ No ☐

   Recommendation: Develop an apartment alert system with neighbors in the complex to help protect each other's property. A well-organized and active tenant association will assist in deterring intruders.

   Recommendation: Get to know the tenants in the complex. After you meet them, make a personal contact list for future use.

4. Does the complex have an electronic access system to control entry into the building? Yes ☐ No ☐

   Recommendation: Do not allow access to strangers by "buzzing" them into the building. If someone enters the building by following you in, and that person is unknown to you, do not ride the elevator with them. If needed, exit the building and then re-enter later.

   Recommendation: Report suspicious strangers, sounds, or actions to police, then notify the complex manager.

MAIL SECURITY

If you receive mail at your home, be wary of suspicious letters or packages. Do not open a letter that appears to be unusual in any way, particularly if it has a perceptible bump, which might be an explosive device. Notify law enforcement immediately of any unexplained package in or near your home. You should notify law enforcement when mail items have any suspicious features, such as:

- Excessive weight, size, or postage
- Springiness in the top, bottom, or sides of the envelope
- Wires or strings protruding from or attached to the envelope
- Envelope has uneven balance or a peculiar odor

- Stiffening of an envelope with cards or other material (such stiffening could be a spring-loaded explosive striker)
- No return address or the place of origin is unusual or unknown
- Name is misspelled

All such items should be isolated. Only trained law enforcement professionals should be allowed to open suspicious mail.

FAMILY SECURITY RECOMMENDATIONS

Recommendation: If at all possible, your home telephone number should be unlisted.

Recommendation: Family members, including care givers, should never tell anyone you are out of the house. They should be instructed to only take messages from callers.

Recommendation: Emergency police and fire numbers should be programmed into the telephone using the "In Case of Emergency" (ICE) concept. If you do not have a programmable phone, you should post emergency numbers near the main telephone in the home.

Recommendation: Do not discuss family plans with outsiders. Even your friends should not be informed. In general, do not discuss your family's comings and goings.

Recommendation: Family members should not stop at the same supermarket at the same time on the same day each week. Vary your daily activities.

Recommendation: Children should be instructed not to open doors to strangers. All visitors should be viewed through a peephole with the door locked. Intercom systems should be used to aid in the identification of strangers.

Recommendation: If it is necessary to leave children at home, keep the house well-lighted and notify the neighbors.

Recommendation: Advise your children to:

- Never leave home without advising parents where they will be and who will accompany them.
- Travel in pairs or groups.
- Walk along busy streets and avoid isolated areas.
- Use play areas where recreational activities are supervised by responsible adults and where police protection is readily available.
- Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot — even if the strangers say mom or dad sent them or said it was okay.

- Report immediately to the nearest person of authority (teacher or police) anyone who attempts to molest or annoy a child.

Recommendation: Be wary of strangers. Be watchful of strange cars that seem to cruise the neighborhood or strange persons who suddenly start to frequent the neighborhood streets. Record information that may be helpful to police.

Recommendation: Observe cars parked in the neighborhood with one or more persons inside or persons who seem to be doing nothing in particular.

Recommendation: Never reveal to any stranger that you are home alone.

Recommendation: Know where your children are at all times. Maintain a daily itinerary and stress the importance of notifying other family members of changes in the schedule.

Recommendation: As mentioned above, have unlisted telephone numbers for ALL family members.

Recommendation: Always request salesmen, repairmen, meter readers, delivery personnel, and even policemen (in civilian clothes) to show their identification prior to admitting them into your home. If in doubt about their identity, place a call to their business to confirm employment. Never accept a phone number that they offer; always use the telephone directory or call the information operator.

Recommendation: Do not put your home telephone number on stationary or on any name and address stickers in order to preclude undesirable telephone calls.

Recommendation: When harassing or obscene telephone calls are received, take action to change your phone number immediately. Family members should never engage in a telephone conversation with unknown or unidentified persons.

Recommendation: Children must follow a school schedule, but if they are driven to school, varied routes should be followed. Children should be escorted to and from bus stops. Neither hiking nor walking to school is recommended.

Recommendation: Inform school authorities that children should not be released from school, athletic events, and club meetings on the strength of a telephone call. Advise the school authorities to confirm the call with your home or office.

Recommendation: Instruct the school administration that if an authorized person does not explain a child's absence from school shortly after school starts, they are to call the child's home or your office to determine the child's status.

Recommendation: Do not open doors to strangers or accept delivery of packages unless the sender is known. Instruct children and in-home help on this procedure. Install a chain

lock on the main entry door so that you may accept small packages or letters by partially opening the door. Do not rely heavily on this type of lock, as an intruder can break them away by forcing the door.

Recommendation: Check references of service personnel, domestics and childcare providers, and any other employees who have routine access to your residence or property.

Recommendation: When receiving a wrong number telephone call, never give your name or number. Just state that the caller has the wrong number.

Recommendation: When a stranger requests to use your telephone for an emergency, never allow entry into the home. Offer to summon assistance, and use the phone yourself.

Recommendation: Never answer your telephone with your name; a simple hello is acceptable.

Recommendation: Report all suspicious activity to the local police.

TRAVEL RECOMMENDATIONS

Whether you are going to the store or Europe, the fact that you have left your home or office changes your security status SIGNIFICANTLY. Travel decreases your security because you are not adhering to your routine, but instead, you are exposed to unfamiliar surroundings. If you plan to travel outside your home area or overseas, you should check with your director of security for additional security measures that can be taken to protect you and your family.

VEHICULAR TRAVEL RECOMMENDATIONS

Recommendation: Do not pick up strangers or give a ride to a stranger or volunteer your car to a group of strangers even though you may have a friend with you in the car.

Recommendation: If you should have car trouble on the road, drive to the side of the road and place a handkerchief or white cloth on the radio antenna or door facing traffic. Either place a cell phone call or wait for help to come.

Recommendation: If you are driving and an attempt is made to force you off the road, move toward the center of the roadway and quickly proceed to a busy street and seek assistance. As you proceed, blow your horn to attract attention to your plight.

Recommendation: Do not stop to aid other motorists or pedestrians, regardless of the circumstances. If you believe the emergency is genuine, use a cell phone or proceed to a public phone and report the matter to authorities, then let them handle the emergency.

Recommendation: If you suspect you are being followed:

- Circle the block to confirm the surveillance.
- Do not stop or take other actions that could lead to a confrontation.
- Do not drive home.
- Do not try to evade or elude the follower.
- Obtain a description of the vehicle and its occupants.
- Go to the nearest police or fire station and report the incident.
- Have an alternative safe place to go in the event you cannot get to the police station.
- Report the incident to police once you are safe.

Recommendation: Avoid using magnetic key boxes hidden in the wheel well of your car.

Recommendation: Park your car in a secured garage; do not park your car on a public street.

GENERAL SECURITY RECOMMENDATIONS

Recommendation: Place the police emergency telephone number (911) and the police non-emergency number next to the phone in your home for immediate use; program it into your telephone system if possible. Do not answer the telephone with your name or official title.

Recommendation: Ladders and scaffolding should be kept in locked outbuildings or garages.

Recommendation: Advise the local police department of your occupation and address. Complete and submit a judicial profile for you and your family (attached), to the chief security officer for use in emergencies. Judicial profiles should be protected as "confidential-restricted access" documents.

Recommendation: Consider moving all fuse and switch boxes into the home if possible. Place locks on those that remain outside or in outbuildings/garages.

Recommendation: Consider a trained watchdog for the family residence. In addition to being a natural deterrent, it is another means of alarming the home.

Recommendation: Be constantly aware of surveillance. Usually a potential victim is watched for several days before an act of violence is carried out.

Recommendation: Prepare an inventory of household and personal possessions, describing the articles and listing the serial numbers for reference.

Recommendation: In order that personal items (jewelry, appliances, TV sets, radios, etc.) can be identified if lost or stolen, a code number should be engraved on each item with an etching machine.

Recommendation: A small safe or security box, which can be bolted down to a closet floor, should be used to secure personal jewelry, cash, and personal documents that are frequently used. Consider a safety deposit box for items used less frequently.

Recommendation: When the home is left vacant, install timers on televisions, radios, and lights in order to give the impression that the home is occupied.

Recommendation: Have "Caller ID" for incoming telephone calls to your home. Use "Caller ID" blocking to prevent your telephone number from being displayed on outgoing calls.

Recommendation: Become familiar with the streets and roads surrounding your home. Have a planned escape route from your home to a designated safe place in case of fire or intrusion.

Recommendation: Plan and practice driving to area emergency services, such as hospitals, police stations, and safe places.

Recommendation: Make sure your trash is kept in a secure place, such as a locked outbuilding.

Recommendation: Keep the names, addresses, and telephone numbers for all staff members handy in the event of an emergency.

Recommendation: If you have household employees, make sure they have been screened with background checks.

For further information contact:
National Center for State Courts
Court Consulting Services
707 17th Street – Suite 2900
Denver, CO 80202
(303) 305-4315

This document was prepared by Jim O'Neil, NCSC Consultant

Revised: February 2009

Appendix D

Model Disaster Recovery Plan Forms

The following section presents sample forms that can be used for the development of a disaster plan regarding the preservations of electronic and hard copies of records in a state court system. The samples contained herein could be made part of pre-service for new employees and in-service training for court staff.

Disaster Planning and Recovery Worksheets

Worksheet Name	Content of worksheet and Instructions	Page
	PRE-DISASTER DOCUMENTATION A set of worksheets should be completed for each court location. This set should be updated annually.	
Emergency Telephone List	Telephone contact for persons and agencies that must be notified of the event	
Disaster Team Assignments	List of names and 24-hour contact information for court disaster team members	
Equipment Supply List	Emergency supplies and equipment	
External Equipment Contacts	24-hour contact information for vendors or others who are able to supply resources or equipment	
Floor Plan	Diagram of the court and/or vault annotated to show the location of computer equipment as well as records	
Records Environment Risk Assessment	A survey of the building, inside and out, especially noting leaks, broken windows and doors, dirt, extraneous materials, damaged furnishings, and other potential hazards	
Evacuation Plan	Security plan to evacuate building, a fundamental part of the court's COOP	
Records Inventory	Inventory of court and administrative records in the area – both electronic and hard copy – including record series titles and dates	
	DISASTER RESPONSE DOCUMENTATION These worksheets are completed during the recovery and salvage process.	
General Procedures During a Disaster	A list of steps to be taken when a disaster occurs for the recovery of both electronic records and hard copy	
Damage Assessment Report	A report used to determine salvage priorities that is composed of a description of the problem created immediately after the event, including an estimate of the scope of the damage, the records involved, and the magnitude of the damage	
Priority Listing	Listing of records to be treated, arranged by priority	
Interim Inventory	A list of the new location of records removed from the usual location for treatment, a list that must be updated as records are treated and returned or marked as unsalvageable	
Disaster Log	Chronological record of actions taken, records involved, and responsible individuals	

Emergency Telephone Numbers

Date completed_____

Form completed by_____

Agency	Contact and alternative if needed	Telephone Numbers
Court Administration		
Police		
Fire Department		
Medical Assistance		
Ambulance		
Other Government Officer		
Maintenance Training and Security Company		
Internet Service Provider		
Judiciary IT Services		
Judicial Security Services		
Disaster Team Leaders		

Disaster Team Assignments and Responsibilities

Date completed_____

Location_____

Team Member Name	Title	Responsibilities	Contact Information
	Team Leader(s)	Individuals with authority to make decisions and to direct others during the disaster and salvage operations. Assign tasks to individuals; perform priority assessment, direct contacts with outside authorities and vendors. Supervise recovery. These individuals are responsible for pre-disaster planning and disaster manual completion for a courthouse. Responsible for the safe evacuation of the building and identification of the location of vital records, both electronic and hard copy.	
	Backup Team Leader(s)	Serves as a back up to the team leader(s) responsible for carrying out leader functions in the absence of the leader. Must have a thorough knowledge of the plan and the resources available.	
	Team Recorder	Team member responsible for completion of logs and documents describing the actions undertaken during the disaster assessment and recovery process**.** This team member is responsible for annotating the movement of records from disaster site to temporary repair location and return.	
	Team Communications Officer	Responsible for communicating information to judges, court personnel, and outside media regarding the status of recovery and the extent of damage of electronic and hard copy records.	
	Team Member	Responsibilities as assigned.	
	Team Member	Responsibilities as assigned.	

External Vendor Contact Information

Date _____

Function or Procedure	Name and Address Contact Person	Telephone or Emergency Access Number
Transport - trucks and equipment to transport boxes of records and/or computer equipment		
Freezer or cold storage location for hard copies		
Freeze-drying contractor for hard copies		
Portable generators to borrow or lease for backup electricity		
Food services (for workers)		
Refrigerated trucks		
Conservationist		
Pest control		
Fumigation services		
Salvage services		
Trash removal		
Alternative location for air drying		
Electrical contractors		
Computer restoration experts		

General Procedures for Hard Copy Records Recovery and Salvage

1. Make sure persons are safe and out of the area.
2. Notify the appropriate persons and agencies of the event. DO NOT try to re-enter a building or handle records until the police and/or fire department indicate that it is safe to enter. Notify the disaster team and administrative officers.
3. Create an assessment report that describes the damage to the structure and materials.
4. Do not remove any records from the area until the priority plan is complete.
5. Create a priority assessment listing the sequence of steps to be taken.
6. Identify a location where records recovery work can take place.
7. DO NOT TRY TO REPAIR RECORDS IN THE DISASTER AREA. All records must be removed to avoid the possibility of additional damage.
8. Try not to exacerbate the damage during the removal process.
9. Document the records being removed. Label the floor plan and note on the disaster log the record type and date, original location, and location in the recovery area.
10. Salvage damaged materials appropriately according to the type of damage.
11. Repair the damaged location.
12. Return materials to the damaged area after inspection.
13. Maintain a disaster log describing actions for future reference.
14. Prepare a disaster report summarizing the event; include advice and analysis of procedures.
15. Replace any emergency equipment or supplies.

Floor Plan

The floor plan of the court should be available in electronic format and in hard copy to help rescue personnel and other professionals physically respond to a disaster or emergency. It should help identify potential problems in addition to providing an overview of the physical layout as well as the location of outlets, master switches, vaults, staircases, windows, and computer equipment. The locations of records, especially confidential and sealed records, should be noted on the plan. The floor plan should be updated annually and copies kept with first responders.

Appendix E

Unified Judicial System of Pennsylvania
Security Incident Fact Sheet

UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

Security Incident Fact Sheet

DISTRICT	02-1-01
DATE OF INCIDENT	March 18 2005
TIME OF INCIDENT	Hour Minutes a.m.

Check Boxes Only Where Applicable

WHAT WAS THE NATURE OF INCIDENT?:

You may choose multiple items from each area below.

You may enter another type of incident by typing a 2- or 3-word description in the "Other" box.

Personal

- ☐ Disorderly Person(s)
- ☐ Physical Assault

Other (Describe below)

Threat

- ☐ Bomb
- ☐ Suspicious Package
- ☐ Verbal

Other (Describe below)

Threat Mode

- ☐ Direct Contact
- ☐ E-mail
- ☐ Mail
- ☐ Telephone

Other (Describe below)

Property Damage

- ☐ Arson
- ☐ Theft
- ☐ Vandalism

Other (Describe below)

Drugs

- ☐ Drugs or Contraband

Other (Describe below)

Emergency

- ☐ Contamination Exposure
- ☐ Explosion
- ☐ Fire
- ☐ Medical
- ☐ Prisoner Escape
- ☐ Weather

Other (Describe below)

WHAT WAS THE EXTENT OF INJURIES?:

- ☐ None
- ☐ Don't know
- ☐ Minor
- ☐ Medical attention required

Description of injuries:

WEAPON INVOLVED?:
You may choose multiple items and/or provide other description.

☐ None	☐ Box cutter	☐ Hands/feet	☐ Razor blade
☐ Biological agent	☐ Chemical agent	☐ Knife	☐ Rifle
☐ Blunt object	☐ Handgun/pistol	☐ Pepper spray	☐ Shotgun

Other: (Describe weapon(s) at right)

IN RELATION TO THE MAGISTERIAL DISTRICT JUDGE COURT FACILITY, WHERE DID THE INCIDENT OCCUR?:
You may choose multiple items and/or provide other description.

☐ Central Court	☐ Garage	☐ Grounds	☐ Staff area
☐ Chambers	☐ Hallway	☐ Lobby	
☐ Courtroom	☐ Holding cell	☐ Parking lot	

☐ Off-site. Indicate address or location. (Describe at right)

WAS AN ALARM ACTIVATED?:

- ☐ No
- ☐ Duress/Panic button
- ☐ Emergency call (911)
- ☐ Magnetometer/X-Ray

Other: What agencies were notified?

WHO WAS INVOLVED IN THE INCIDENT?:
You may choose multiple individuals and write in any not listed.

☐ Magisterial District Judge	☐ Prosecutor	☐ Security officer	☐ Defendant
☐ Court Staff	☐ Constable	☐ Sheriff	☐ Plaintiff
☐ Defense counsel	☐ Municipal police	☐ State police	☐ Prisoner
			☐ Member of public

Other (Describe at right)

Were any of the persons involved in the incident attending a court proceeding? ○ Yes ○ No

If yes, what type of case?

☐ Civil Case ☐ Landlord/tenant ☐ Private Criminal Complaint ☐ Non-traffic Citation
☐ Criminal Case ☐ Protection From Abuse ☐ Traffic Citation

Case Caption (Enter at right)

If known, enter names of those involved. Enter number of names then click update.

Update

SUMMARY OF FACTS:
Please include the name of each agency that responded to the incident (e.g., sheriff, state police, fire department) as well as the circumstances leading up to the event.

NAME OF INDIVIDUAL FILING THIS REPORT: Larry C. Kerr

Did you personally witness the incident? ○ Yes ○ No

If you answered No above, enter the name of the person for whom you are filing this report:

Last name: First name: Middle initial: Name suffix: (Jr., Sr.)

REPORT FILING OPTIONS

Save until I return and complete the report
(Allows you to return and edit this report within the next 7 days. This option is useful if you cannot complete the report at this time.)

Save and return

OR

Save the report for the record
(This option will submit the report immediately. You will not have the option of editing this report at a later time.)

Save for the record