

C O U R T • H O U S E

COURT SECURITY GUIDE

Revised June 2024



**National Association
for Court Management**

National Association for Court Management

Communications Committee

Dawn Palermo, Chair
Louisiana

Nathaniel Mingo, Vice Chair
Georgia

Security Guide Subcommittee

Nathaniel Mingo, Chair
Georgia

Jonathan Gadberry
Oregon

Brian Wiggins
Louisiana

Damon Anderson
Louisiana

Robert Gunn
Louisiana

Audrey Anger
Kansas

Tim Leger
Louisiana

Randy Swope
Oregon

Bo (George) Coxen
Louisiana

Evan West
Oregon

Special thanks to:

Robert Granzow, Pennsylvania

Mary Hughes Coleman, Riverdale

2023-2024 Board of Directors

PRESIDENT
Rick Pierce

PRESIDENT ELECT
Tina Mattison

VICE PRESIDENT
Kelly Hutton

SECRETARY/TREASURER
Greg Lambard

IMMEDIATE PAST PRESIDENT
Jeffrey Tsunekawa

DIRECTORS

Kristie Collier
Brandon Kimura
Dawn Palermo
Cheryl Stone

Nicole Zoe García
Nathaniel Mingo
Roger Rand
Creadell Webb



Table of Contents

Chapter 1: Introduction	1
I. Responsibility	2
II. A Security Plan	5
Chapter 2: Understanding Current Threats and Trends	7
Chapter 3: Updating Policies and Procedures	9
Screening Protocols	9
Emergency Response Plans	10
Physical Security Measures	11
Chapter 4: Leveraging Technology Advances	11
Biometric Authentication Systems	11
Video Surveillance Technologies	12
Threat Detection Software	13
Chapter 5: Enhancing Emergency Preparedness	13
Risk Assessment	14
Training and Drills	14
Communication and Coordination	14
Chapter 6: Ensuring Accessibility and Inclusivity	15
ADA Compliance	15
Design Considerations	16
Alternative Accommodations	17
Chapter 7: Engaging Stakeholders and Training Resources	17
Collaborative Partnerships	17
Security Awareness Training	18
Professional Development Opportunities	18
Chapter 8: Special Situations	19
A. High-Profile Cases	20
B. Sequestered Juries	20
C. High-Security Cases	22
D. Demonstrations	23
E. Medical Emergency	24
F. Pandemics	25
G. Evacuation	26

H. Workplace Violence	26
I. Fire	26
J. Hostage	27
K. Bomb	27
L. Mail	28
M. Terrorism	28
N. Cyber Attacks	28
Chapter 9: Conclusion	29
APPENDIX A	31
Areas of Concern in a Security Survey	31
Appendix B	33
Courtroom or Courthouse Security Order	33
Appendix C	34
Instructions for Bailiffs Guarding Sequestered Jurors	34
Appendix D	36
Bomb Threat Checklist	36
Appendix E	37
Emergency Action Plan	37
Appendix F	52
The Pennsylvania Judicial Incident Reporting System (PAJIRS)	52

Chapter 1: Introduction

In the 21st century and beyond, court security has become an increasingly important aspect of the criminal justice system. With the rise of global terrorism, cyber threats, and civil unrest, ensuring the safety and security of courthouses and the individuals within them has become a top priority for judicial authorities. This guide will explore the various dimensions of court security in the contemporary era, including physical security measures, technological advancements, personnel training, and the challenges posed by evolving threats.

To understand the current state of court security, it is essential to examine its historical evolution. Throughout history, courts have been the focal points of public scrutiny, legal disputes, and societal tensions. As such, they have always been vulnerable to security threats, ranging from physical violence to organized attacks. The assassination of President Abraham Lincoln in Ford's Theatre in 1865 and the bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995 as well as the horrific events that occurred in the Fulton County Courthouse in 2005 when Brian Nichols went on his rampage and most recently a Maryland Judge gunned down in his driveway serve as poignant reminders of the potential dangers faced by court facilities and court staff.

In response to these threats, the concept of court security has evolved from a rudimentary system of guards and metal detectors to a sophisticated network of measures designed to protect court personnel, litigants, and the public. The 21st century has witnessed a paradigm shift in the approach to court security, driven by technological advancements, intelligence gathering, and strategic planning.

The adoption of access control systems, biometric authentication, and smart card technology has enhanced the ability to manage and restrict entry to sensitive areas. These systems not only prevent unauthorized access but also generate audit trails that can be invaluable for forensic investigations and post-incident analysis.

This guide is primarily a checklist rather than a blueprint. The process involves identifying and proposing solutions to problems. Each court is then required to create its own detailed plan that is tailored to its local environment, culture, and requirements. The most effective security measures are those that are always watchful, thorough, somewhat concealed, and never assumed to be sufficient. This guide is provided to aid courts in achieving those objectives.

I. Responsibility

The responsibility for securing physical and virtual courthouses is both focused and general. The ultimate authority for courthouse security usually is focused by law or practice on one person. Either way, it is best that one person has the final responsibility. Whether the chief judge, the sheriff, or the court administrator, this person's mission is three-fold: to match resources with need; to set policy goals and monitor the degree to which those goals are met; and to create awareness on the part of all those working in and entering the courts about the need to maintain a secure facility and infrastructure.

In some jurisdictions, physical security is the legal responsibility of a sheriff or law enforcement local police department, but the judges and court employees expect the court administrator to be knowledgeable and involved, at least at the policy level. In such cases, the administrator should establish regular communication with the legally responsible entity and expect an equal role in setting policy and approving the security plan. Large courts often appoint a security liaison to interface with the security agency daily.

Courts often share facilities with other government agencies. Building-wide security may be possible in these circumstances, but it may not be. In the latter instance, security for the court's portion of a building has to be provided within the context of a building that is not secure. The ultimate responsibility for court security would not change, but the approach needs an additional element. A coordinating committee consisting of representatives of all entities in the building is essential for effective security. This committee can assist in developing and overseeing the security plan and ensure that other tenants in the building know the court's needs and plans. It also allows the other entities to develop their plans if a security incident in the court impacts other parts of the building.

The cybersecurity of the court traditionally falls on the IT Director, technology chiefs, or emergency management personnel, but the court administration must understand the necessary components and threats. Court Administration will be expected to budget, acquire, and coordinate cybersecurity technology with the assistance of the IT Director. Regular communication between court administration and IT is vital for success. The Court Administrator will need to ensure that staff and court computer system users are thoroughly trained to know the dangers and threats to the system. Court leadership must establish and enforce Cybersecurity procedures and protocols to minimize risks and disseminate those procedures and protocols to staff.

Emergency management personnel also play a central role in preparing for and responding to cybersecurity incidents in their jurisdiction. The court administration must plan cybersecurity preparation accordingly with emergency management departments. Although emergency managers and court administrators are not expected to be technical experts on cybersecurity incidents, they need to understand and prepare for the potential impacts of a cybersecurity incident.

All court employees share responsibility for security. For both physical and cyber security, employees must know what is common and uncommon so that when they observe public and work areas that may not be monitored by security personnel, they may be in the best position to see suspicious behavior by visitors or litigants. They may be immediately affected by a security incident. It should be reasonably easy, therefore, to get staff's support and assistance. Staff are the greatest risk to a cyber system because their incorrect click could open the court data system to invaders. Continuous training of staff on cyber threats and how to react is extremely important.

Rarely should exceptions and deviations to policies and procedures be allowed. Staff need clear guidance to follow security best practices and assist the public. Staff need to understand the expectations and policies should be regularly reviewed with staff and placed in the employee handbook or business continuity of operations plan (COOP).

Placing the burden solely on staff has potential pitfalls. First, complacency may set in. If security is everyone's concern, it may become no one's concern, as each person becomes convinced another will do the job. Equally risky, if there are no incidents over months or even years, staff may come to believe that none will occur; the institution might be most vulnerable when staff come to believe

security is unneeded. Also, employees may not feel comfortable with the idea that they bear some burden for security, feeling it should rest with trained professionals. The issue of consciously or unconsciously deferring responsibility to others should be addressed through training programs involving both court management and trained security personnel. The training must emphasize that responsibility for a secure environment is shared with those in law enforcement or protection management and that only constant vigilance, even in extended times of quiet, assures security. In addition, cybersecurity is ever evolving so training must occur regularly and possibly through phishing exercises and skills testing to ensure staff understands what to look for.

Those who enter the courthouse on a regular basis (such as attorneys), from time to time, (law enforcement, social service agency personnel, a variety of others), or even rarely (public) can also assist with security. Their responsibility and the capacity to inform, however, is limited. Security personnel and employees can create an atmosphere indicating a security consciousness that sensitizes the public. The “atmosphere” can be reinforced by signs asking people who see a suspicious package to contact security or a member of the court’s staff or in the relatively simple placement of a secure phone and contact numbers throughout the building. For the Bar, letters from the chief administrative judge and/or occasional comments at Bar meetings can reinforce the need for all to be alert.

For cybersecurity, staff should be trained to pause, reflect upon their cybersecurity training, and ask questions or call their IT department before responding to questionable suspicious electronic requests. Unique or differing requests are better reviewed by a different more technical set of eyes than responding and jeopardizing the safety of the system. Staff should be encouraged to be safe and question items no matter how great the matter is or isn’t. Failure in cybersecurity can cripple the court for hours, days or even, weeks, and sometimes months! Even with the best cybersecurity program in place. Cyber cybersecurity incidents are always a risk.

II. A Security Plan



What is a security plan?

Many states by statute or court rule require the development of a security plan, and a cyber assessment plan. A security plan has two purposes: a general guide for staff and policy makers and an operation manual for security personnel. It displays how the court will address specific issues, particularly those discussed in this guide. A security plan need not be massive. Instead, in the most concise manner possible, it should advise staff and judicial officers how to prevent security incidents and what to do should they occur. A second volume or appendices can provide the myriad details for scenarios that the court's security department would need to know but staff would not.

The plan should address three elements of securing the court and those who use it:

- Daily, general securing of the facility;
- Procedures for handling continuing security concerns such as prisoner transport, the theft of documents or personal items, and minor medical emergencies; and
- Contingency plans for major security concerns such as hostage situations, weapons use, bomb threats, fights, demonstrations, major medical conditions, fires, special high-security defendants and notorious cases.

Within these three elements, there are three areas to consider:

- Operations;
- Technology; and
- Architecture.

Cybersecurity is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

A cybersecurity plan requires training of staff and court computer system users.

The plan also requires appropriate cyber monitoring equipment, software and regular updates (patterns) of critical



systems. Many states now require that agency staff have a minimum of 1 hour of cybersecurity training annually. The requirement is tested in the financial audit. Guidance from the Federal Emergency Management Agency (FEMA) and Cybersecurity and Infrastructure Security Agency (CISA)

can be used to assist in plan development (Visit www.CISA.GOV). The goal of cybersecurity is to stop or minimize disruptions.

Part of a cybersecurity plan should include a section on the court's cyber incident response plan. This plan enables the organizations to act quickly when attacked. The plan helps mitigate impacts and returns functionality as soon as possible. Most cyber incident response planning occurs before an incident and in conjunction with a cybersecurity plan.



A cybersecurity plan should include:

- Identification of cyber response team members;
- Cyber incident response planning and procedures;
- Cybersecurity technology requirements;
- Cybersecurity training plan; and
- Post-incident processing steps.

Preparation is the key to success. According to the FBI's 2022 Internet Crime report, the top three Critical Infrastructure Sectors victimized by ransomware were:

1. Healthcare and Public Health;
2. Critical Manufacturing; and
3. Government Facilities.

Cybersecurity is vital for all courts because without it, court operations could cease rendering all court computers and servers inoperable, shut down courts for hours or days, and personal identifiable information (pii) could be released.

Chapter 2: Understanding Current Threats and Trends

In today's rapidly changing landscape, court security professionals must remain vigilant in identifying and addressing evolving threats and trends. This chapter provides an overview of the current threats and challenges facing court security, including:

- **Cyber Threats:** With the increasing digitization of court operations, cyber threats pose a significant risk to court systems. Hackers may target court databases, case management systems, and online portals, compromising sensitive information and disrupting court proceedings. Cyberattacks such as ransomware, phishing, and data breaches can have severe consequences for court operations, including monetary loss, reputational damage, and compromised data integrity. Court administrators must implement robust cybersecurity measures to safeguard court systems and data including encryption, multi-factor authentication, and regular security audits. Over the last 10 years, the occurrence of malware attacks and network hijackings have increased in severity. While courts have been striving to embrace the digital age that has been brought in by computers, smart phones, and personal electronic devices, the very nature of these devices has exposed the court and its information to dangerous elements of society. We have seen networks and network systems frozen until a payment of some sort can be made. To combat these elements, courts

are being forced to allocate money and resources into their infrastructure to minimize the occurrence of an attack. The idiom “It’s not a matter of if but when” has become the realization of today’s digital world. Court Administrators must always be able to accept pleadings and filings from defendants and attorneys alike but must also be on the defensive that a trojan hijacker or malware is not being inserted into their networks. Training of court staff is required to ensure safe internet hygiene. Firewalls are needed to protect networks and their computers. States are adding cybersecurity training to their required certifications.

- **Terrorism Concerns:** Courts may be targeted by extremist groups or individuals seeking to incite fear, disrupt the judicial process, or advance their agendas. Administrators must be prepared to respond swiftly and effectively to potential acts of terrorism, implementing robust security measures to prevent and mitigate threats. Threats of violence, bombings, and attacks on judges, prosecutors, and other court personnel require heightened vigilance and coordination with law enforcement agencies and intelligence services. Court administrators should conduct threat assessments and vulnerability analyses to identify potential targets and security gaps, implementing appropriate measures to deter and mitigate terrorist threats.
- **Civil Unrest:** Social unrest, protests, and demonstrations can pose security challenges for court facilities, particularly in cases involving high-profile trials or controversial verdicts. Administrators should monitor developments in their communities and collaborate with law enforcement agencies to maintain order and ensure the safety of court personnel and visitors. Protests related to issues such as racial justice, police brutality, and immigration policies have escalated into violence or disruptions, necessitating proactive security measures and contingency planning. Court administrators should establish communication protocols with local law enforcement agencies and community leaders to facilitate timely information sharing and coordination during periods of civil unrest.



By understanding these threats and trends, court administrators can develop proactive strategies to enhance security measures, strengthen resilience, and safeguard the integrity of the judicial process.

Chapter 3: Updating Policies and Procedures

Effective security starts with clear policies and procedures that reflect the current court security practices. This chapter outlines key considerations for updating policies and procedures, including:

Screening Protocols

Implementing robust screening protocols at the front/main entrance(s) is essential for preventing weapons, contraband, and other prohibited items from entering court facilities. Administrators should review and update screening procedures to incorporate the latest technologies and best practices, such as metal detectors, X-ray scanners, and explosive detection systems. Screening procedures should be tailored to each court facility's specific needs and risk

profiles, considering factors such as caseload, facility layout, and threat assessment. Administrators should also consider the use of behavioral detection techniques and non-intrusive screening methods to enhance detection capabilities while minimizing inconvenience to court users.



Emergency Response Plans

Preparedness is paramount in responding to emergencies, including natural disasters, acts of violence, and other crises. Administrators should review and revise emergency response plans to address emerging threats and ensure coordination with local law enforcement, emergency services, and other stakeholders. Emergency response plans should include procedures for evacuations, sheltering in place, lockdowns, and communication with court personnel, visitors, and external stakeholders. Regular drills and exercises are essential for testing and refining emergency response procedures, identifying gaps and areas for improvement, and familiarizing court personnel with their roles and responsibilities during emergencies. Court personnel should also be aware of emergency equipment locations and alarm systems. Administrators should also consider incorporating provisions for psychological first aid and trauma-informed care into emergency response plans, recognizing the potential impact of traumatic events on court personnel and visitors.

Physical Security Measures

Enhancing physical security measures is critical to deterring unauthorized access, protecting sensitive areas, and safeguarding court personnel and visitors. Administrators should assess the effectiveness of existing security measures, such as access control systems, perimeter fencing, and surveillance cameras, and make necessary upgrades to address vulnerabilities and mitigate risks. Physical security measures should be integrated with other security layers, such as screening protocols and emergency response plans, to create a comprehensive security framework that addresses multiple threats and scenarios. Administrators should also consider the use of crime prevention through environmental design (CPTED) principles to enhance security and create a welcoming environment for court users. CPTED strategies include maximizing natural surveillance, controlling access points, and creating well-lit and aesthetically pleasing spaces that discourage criminal activity.

By updating policies and procedures in accordance with current best practices and standards, court administrators can strengthen security protocols, minimize vulnerabilities, and promote a safe and secure environment for all.

Chapter 4: Leveraging Technology Advances

Advancements in technology play a pivotal role in enhancing court security and efficiency. This chapter explores the latest innovations and trends in security technology, including:

Biometric Authentication Systems

Biometric technologies, such as fingerprint scanners, facial recognition systems, and iris recognition technology, offer secure and convenient authentication

solutions for controlling access to court facilities and sensitive areas. Biometric authentication systems provide greater accuracy and reliability than traditional



methods, such as passwords and access cards, reducing the risk of unauthorized access and identity fraud. Administrators should evaluate the suitability of biometric authentication systems for their court facilities, considering factors such as cost, usability, and privacy implications. Biometric data should be securely stored and encrypted to protect individuals' privacy rights and comply with data protection regulations. Administrators should also ensure that biometric systems are accessible to individuals with disabilities and do

not discriminate based on race, gender, or other protected characteristics.

Video Surveillance Technologies

Video surveillance technologies enhance situational awareness and investigative capabilities. These technologies include high-definition video surveillance cameras, networked video management systems, and intelligent video analytics enable real-time monitoring, event detection, and forensic analysis of security incidents. Video surveillance technologies can deter criminal activity, provide evidence for prosecution, and facilitate post-incident analysis and



reporting. Administrators should deploy video surveillance cameras strategically throughout court facilities, focusing on critical areas such as entrances, lobbies, courtrooms, and holding areas. Video surveillance systems should comply with privacy regulations and ethical standards, balancing security needs with individuals' rights to privacy and due process. Administrators

should also consider the use of video analytics tools, such as facial recognition and object detection algorithms, to enhance the effectiveness of video surveillance systems and automate security monitoring tasks.

Threat Detection Software

Advanced threat detection software utilizes artificial intelligence, machine learning, and data analytics to identify and mitigate potential security threats, such as suspicious behavior, unauthorized access attempts, and anomalous activities. Threat detection software can analyze large volumes of data from multiple sources, including video surveillance cameras, access control systems, and cybersecurity tools, to detect patterns and anomalies indicative of security risks. Administrators should integrate threat detection software with other security systems and protocols to create a layered defense strategy that detects, analyzes, and responds to security threats in real time. Threat detection algorithms should be continuously updated and refined based on feedback from security personnel and evolving threat landscapes. Administrators should also consider the use of threat intelligence platforms and information sharing networks to stay abreast of emerging threats and trends, enabling proactive threat mitigation and risk management.

By leveraging technological advances, court administrators can strengthen security measures, streamline operations, and improve overall safety and efficiency now and beyond.

Chapter 5: Enhancing Emergency Preparedness

Preparation is essential for effectively responding to emergencies and crisis situations. This chapter provides guidance on enhancing emergency preparedness and response capabilities, including:

Risk Assessment

Conducting a comprehensive risk assessment helps identify potential threats, vulnerabilities, and critical assets, enabling administrators to prioritize resources and develop targeted mitigation strategies. Administrators should consider a wide range of hazards and scenarios, including natural disasters, technological failures, criminal activity, and terrorist attacks. Risk assessments should involve input from internal and external stakeholders, including court personnel, security professionals, and emergency responders, to ensure a comprehensive and accurate understanding of security risks. Administrators should also consider conducting vulnerability assessments and scenario planning exercises to simulate potential security threats and evaluate the effectiveness of existing security measures.

Training and Drills

Regular training sessions and emergency drills familiarize court personnel with emergency procedures, roles and responsibilities, and communication protocols, ensuring a coordinated and effective response in times of crisis. Training programs should cover a wide range of topics, including threat recognition, emergency response procedures and conflict resolution techniques. Practical exercises and simulations provide hands-on experience and reinforce key concepts, helping to build confidence and resilience among court personnel. Administrators should also consider incorporating cross-training initiatives and multi-disciplinary training exercises to enhance collaboration and coordination between different departments and agencies involved in emergency response efforts.

Communication and Coordination

Clear lines of communication and coordination with internal and external stakeholders, including law enforcement agencies, emergency services, and community partners, should be established to facilitate timely information sharing and collaboration during emergencies. Administrators should develop

communication protocols and contingency plans for different types of emergencies, ensuring redundancy and resilience in communication systems. Regular drills and tabletop exercises help identify communication gaps and challenges, allowing administrators to refine communication strategies and improve response coordination. Administrators should also leverage technology tools, such as mass notification systems and emergency communication apps, to disseminate critical information and instructions to court personnel and visitors during emergencies.

By enhancing emergency preparedness efforts, court administrators can mitigate risks, minimize disruptions, and ensure the safety and well-being of all stakeholders in the event of an emergency.

Chapter 6: Ensuring Accessibility and Inclusivity

While maintaining security is paramount, it is also essential to ensure accessibility and inclusivity for all court users, including individuals with disabilities. This chapter explores strategies for balancing security needs with accessibility requirements, including:

ADA Compliance

Ensuring compliance with the Americans with Disabilities Act (ADA) and other accessibility standards is essential for accommodating individuals with disabilities and promoting equal access to court facilities and services. Administrators should conduct accessibility audits and assessments to identify barriers and deficiencies in court facilities, such as inaccessible entrances, narrow doorways, and inadequate signage. Remediation plans should prioritize barrier removal and accessibility improvements to enhance the usability and inclusivity of court facilities for individuals with disabilities. Administrators should also consider the

use of universal design principles and user-centered design approaches to create accessible and inclusive environments that accommodate a wide range of abilities and preferences.



Design Considerations

Incorporating universal design principles, such as wheelchair ramps, accessible entrances, and tactile signage, enhances the usability and inclusivity of court facilities for individuals with disabilities. Administrators should consult with accessibility experts and disability advocates to incorporate user-centered design features that accommodate a wide range of abilities and preferences. Design considerations should address physical, sensory, and cognitive impairments, ensuring that court facilities are welcoming and accessible to all. Administrators should also consider the use of assistive technologies and adaptive equipment, such as hearing loops, screen readers, and mobility aids, to enhance accessibility and facilitate participation for individuals with disabilities. Consideration of changes in court security must be reviewed. Alternative security measures may need to be designed.

Alternative Accommodations

Providing alternative accommodations facilitates effective communication and participation for individuals with disabilities. Alternative forms of accommodation include sign language interpreters, assistive listening devices, and accessible court documents formats. Administrators should establish protocols for requesting and providing accommodations, ensuring timely and equitable access to court proceedings and services. Training court personnel in disability etiquette and best practices promotes sensitivity and awareness of individuals' needs and preferences. Administrators should also consider the use of remote access technologies, such as video conferencing and telepresence systems, to provide virtual accommodations for individuals who are unable to attend court in person due to disability-related barriers or other circumstances.

By prioritizing accessibility and inclusivity, court administrators can create a welcoming and inclusive environment that respects the rights and dignity of all court users.

Chapter 7: Engaging Stakeholders and Training Resources

Effective court security management requires collaboration and cooperation among multiple stakeholders. This chapter discusses the importance of engaging stakeholders and providing training resources to enhance security awareness and preparedness, including:

Collaborative Partnerships

Building collaborative partnerships with law enforcement agencies, government agencies, community organizations, and other stakeholders is vital. These partnerships foster information sharing, resource sharing, and coordinated efforts

to address security challenges. Administrators should establish formal partnerships and working groups to facilitate ongoing communication and collaboration on security-related issues. In addition to the court security team meetings, joint training exercises, information sharing forums, and task forces provide opportunities for stakeholders to exchange knowledge and expertise, identify common goals and priorities, and develop coordinated strategies to address shared security concerns. Administrators should also consider establishing community advisory boards or security committees to solicit input and feedback from key stakeholders and community members on security-related matters.

Security Awareness Training

Providing security awareness training for court personnel, security personnel, and other stakeholders increases awareness of security threats, promotes vigilance,



and empowers individuals to take proactive measures to enhance security. Training programs should cover a wide range of topics, including threat recognition, emergency response procedures, conflict resolution techniques, and cybersecurity best practices. Interactive and scenario-based training modules engage participants and reinforce key concepts, helping to build

a culture of security throughout the organization. Administrators should also consider providing specialized training for frontline staff, security officers, and other personnel responsible for implementing security protocols and procedures.

Professional Development Opportunities

Offering professional development opportunities, such as workshops, seminars, and certification programs, enables court personnel and security professionals to enhance their knowledge, skills, and competencies in court security management. Administrators should support ongoing professional

development for staff members by providing access to relevant training resources, funding opportunities, and career advancement pathways. Professional development programs should be tailored to the specific needs and interests of participants, addressing emerging trends, evolving technologies, and changing regulatory requirements in court security management. Administrators should also encourage staff members to pursue professional certifications and credentials in areas such as security management, emergency preparedness, and risk assessment to enhance their expertise and credibility in the field.

By engaging stakeholders and investing in training resources, court administrators can strengthen relationships, foster a culture of security, and build capacity to address evolving security challenges.

Chapter 8: Special Situations

Several extraordinary circumstances or emergency events can occur for which the court should have a plan in place. These events include high-profile cases, high-security situations, demonstrations, and emergencies requiring evacuation, such as workplace violence, fire, bomb threats, and hostage situations. There should also be plans in place for mail safety and terroristic threats.

To ensure that emergencies are handled calmly and efficiently, the court should conduct periodic drills. The plans should include provisions for disabled individuals. Emergency policies should also consider responsibility for witnesses, jurors, counsel, and the public, in addition to the safety of staff and judicial officers. Review of the plan by the fire marshal is advisable to address potential conflicts between fire safety regulations and security policies.

A. High-Profile Cases

A high-profile case can arise suddenly, requiring a swift and responsible response from the court to protect its staff and facilities. Characteristics associated with such cases include multiple victims, incidents involving female victims and multiple offenders, and homicides involving intimate or family relationships. Cases involving celebrity defendants or child victims may garner national attention.

High-profile cases can lead to increased public presence in and around the courthouse, along with heightened media interest. Separate media facilities may be necessary, even if proceedings are televised live. The court should anticipate larger crowds and potential security concerns both inside and outside the courthouse. Early coordination with local law enforcement is crucial.

B. Sequestered Juries

Sequestered juries require special attention and increased security. The general instructions for sequestering will list duties of bailiffs and court security. Such duties include, but are not limited to:

- The management of the sequestration hotel should be instructed that all telephone calls are to be diverted to the bailiff or court security personnel rooms.
- Any telephone calls made by any juror or received by any juror shall be monitored by the bailiff or other court security personnel and logged. Jurors may not possess mobile or cell phones.
- Jurors shall not be permitted to make or receive telephone calls without the express knowledge of the bailiff or other court security personnel supervisors.
- The bailiff and court security personnel shall seat themselves in such a way as to monitor any contact with non-jurors and jurors during meal periods. Further, court security personnel and the bailiff shall not sit with the jurors and converse with them during meals.

- The court bailiff and security personnel shall establish an emergency evacuation procedure for the swift and safe movement of jurors from the hotel, restaurant or other area, if necessary.
- The television or recreation room shall be monitored at all times by a court security personnel or the bailiff and all programming shall be pre-approved by waitresses, vehicle drivers, or others will be instructed not to hold any unnecessary conversation with members of the jury. Any video tapes used shall be pre-approved by the judge for use in the television lounge area.
- Bailiff and court security personnel shall prepare and complete a check list on each room indicating that proper measures have been completed to protect the sequestering of the jury. Jurors' rooms will be re-checked prior to the jurors' return to the rooms.
- At least one member of the court's security personnel shall be on duty at all times at the jury sequestering site even while jurors are at meals, etc. All rooms must be secured by appropriate personnel to maintain the integrity of the jury.
- All persons entering the floor where the juror have been sequestered shall be logged in and out and accompanied by court security personnel at all times.
- During deliberations, there will be at least one member of the court's security staff posted outside of the jury deliberation room. At no time shall the court security staff member enter the jury room during deliberations. Any requests from the jury shall be reported immediately to the trial judge or to the bailiff.
- During transportation of jurors, the route of travel should be known to all court security personnel. Areas in the route of travel, in particular, if the route of travel will involve walking, shall be checked so that jurors will not be permitted to view newsstands or coin operated newspaper dispensers.
- Any juror that wishes to smoke or obtain any type of recreational activity shall be accompanied at all times by a member of the court security personnel.
- Court security should be stationed at each end of the suite of juror rooms for total security. Juror rooms should, if possible, be located on one wing of the particular hotel so that security may be handled on a more complete

basis. Each juror shall have a private room and at least one common television recreation room should be provided.

- Any incident of any nature should be reported in an incident report and the trial Judge should be immediately notified. No juror is to leave the sequestered area without court security personnel accompanying the juror at all times.
- Court security personnel should be discouraged from having personal discussions with jurors during the sequestering process. Advise security personnel to never discuss the case under any circumstances with a juror.
- Court security personnel should be advised to act as security personnel and not as companions of the jurors during the sequestering process. This should be explained to jurors prior to the sequestering process by the trial judge.
- Court security personnel should set up an appropriate wake up procedure to knock on all jurors' doors on at least two occasions to advise them of wake-up time and to call them again prior to accompanying all jurors to the breakfast area. Should any juror stay behind and not attend breakfast, court security personnel must stay in the vicinity of that juror to protect the sequestering process.
- The juror sequestering personal information forms are to be completed and held by security at all times and transported with the jury at all times. Security should always have these forms immediately available.

C. High-Security Cases

Even before 9/11, courts faced security challenges related to high-profile individuals, such as political figures, celebrities, or individuals associated with notorious cases. However, in recent years, the security landscape has been further complicated by the presence of prominent public figures like Donald Trump, the former President of the United States.

Cases involving individuals of significant public interest, such as Trump, often attract potential security risks. Given the polarizing nature of such figures, court proceedings involving them may necessitate additional security measures to

ensure the safety of all involved parties and maintain the integrity of the judicial process.

Security protocols for high-profile cases may include increased presence of uniformed and plainclothes security personnel, enhanced perimeter security measures, and specialized arrangements for protecting jurors, witnesses, and other participants. Moreover, the courtroom and courthouse infrastructure may require modifications to accommodate the heightened security needs associated



with high-profile cases. This could involve implementing secure access controls, installing surveillance systems, and establishing secure areas for sensitive proceedings.

Additionally, courts must remain vigilant against potential threats posed by extremist groups or individuals seeking to exploit high-profile cases for disruptive or violent purposes. Collaborating closely with federal, state, and local law enforcement agencies is essential to assess and mitigate these risks effectively.

Considering these challenges, courts must develop comprehensive security plans that include conducting risk assessments, scenario planning, and regular security drills to ensure preparedness for any eventuality. By prioritizing the safety and security of all individuals involved in high-profile cases, courts can uphold the principles of justice, protect the rule of law, and maintain public trust in the judicial system.

D. Demonstrations

Demonstrations pose unique challenges for court security which require careful consideration of location, scale, and potential disruptions to court proceedings. While demonstrations inside courtrooms or courthouses are typically prohibited, those occurring outside may be subject to court orders or limitations as part of the security plan.

The response to demonstrations hinges on their location and demeanor. Coordination with local law enforcement is essential both in planning and during a demonstration to ensure the safety of all involved.

Inside the courthouse, security personnel must be prepared to enforce court orders regarding demonstrations and, if necessary, initiate evacuation procedures to maintain order and safety. For demonstrations immediately outside courthouses, security protocols should include provisions for managing crowd control, monitoring for potential disruptions, and implementing evacuation plans if needed.

In cases where demonstrations escalate into disturbances, court security must be prepared to swiftly and effectively respond, ensuring the safety of court personnel, visitors, and property.

Communication between court security, law enforcement, and relevant stakeholders is paramount to coordinate response efforts and mitigate potential risks posed by demonstrations.

As part of the court's overall security plan, ongoing training and preparedness exercises should be conducted to equip staff with the skills and knowledge necessary to respond effectively to demonstrations and maintain the integrity of court proceedings.

By proactively addressing the security implications of demonstrations and collaborating closely with law enforcement partners, courts can minimize disruptions and uphold the rule of law in the face of public demonstrations.

E. Medical Emergency

Medical emergencies present security-related concerns, often requiring intervention by outside emergency personnel. Pre-existing agreements with local emergency services should be in place. Court staff should be trained in first aid and CPR, and medical equipment should be readily available. Staff should be aware of the location of medical equipment (such as AED or Narcan) and how to access such equipment. Staff should prioritize contacting internal security personnel in case of a medical emergency.



F. Pandemics

The emergence of pandemics, such as the COVID-19 outbreak, has reshaped the landscape of court operations and necessitated significant adaptations in judicial procedures. These global health crises disrupt normal functioning, prompting courts to implement innovative measures to ensure the continuity of justice while prioritizing public health and safety.

The COVID-19 pandemic, which unfolded between 2020 and 2021, forced courthouses worldwide to shutter their doors temporarily to mitigate the spread of the virus. In response, courts swiftly transitioned to remote proceedings, leveraging technology to conduct hearings, trials, and other legal proceedings virtually. Hybrid work environments became commonplace. Court staff would alternate between remote, and in-person work to minimize the risk of transmission. Video conferencing tools replaced traditional courtroom proceedings, enabling attorneys, witnesses, and other stakeholders to participate remotely while maintaining social distancing protocols.

The pandemic underscored the importance of flexibility and adaptability in court operations. Courts developed comprehensive protocols for remote proceedings, including guidelines for conducting virtual hearings, filing documents electronically, and ensuring secure communication channels.

As the threat of pandemics persists, courts continue to refine their response strategies to future outbreaks. This includes investing in robust technology infrastructure to support remote proceedings, enhancing cybersecurity measures to protect sensitive data exchanged online, and providing ongoing training to court personnel on remote proceedings protocols.

Courts are also exploring innovative solutions to address the backlog of cases accumulated during the pandemic, such as alternative dispute resolution mechanisms and expedited case processing. These initiatives aim to ease the strain on court resources and expedite the resolution of legal disputes quickly.

Ultimately, pandemics serve as catalysts for transformative change in court operations, prompting courts to embrace technology, streamline processes, and prioritize resilience in the face of unprecedented challenges. By leveraging lessons learned from past pandemics, courts can better prepare for future health crises and ensure the uninterrupted administration of justice.

G. Evacuation

Evacuation procedures should be in place for various emergencies, including fire, bomb threats, or natural disasters. Plans should cover communication protocols, evacuation routes for staff and the public, procedures for prisoners and jurors, and maintaining the integrity of evidence. Regular drills and audits are essential to identify and address potential hazards.

H. Workplace Violence

Workplace violence policies should articulate zero tolerance for such incidents and include procedures for reporting and responding to threats or violence. Staff should receive training in identifying and handling potential threats.

I. Fire

Security policies should include procedures for reporting fires, contact with local fire departments, and staff training in using fire extinguishing equipment. Regular drills and inspections are necessary to ensure staff are familiar with evacuation procedures and fire safety protocols.



J. Hostage

Hostage situations require professional handling by law enforcement personnel. Court security personnel should be trained in responding to such situations and coordinating with law enforcement agencies. Staff and judicial officers should be provided with guidance on how to respond if taken hostage.

K. Bomb

Courts should have procedures in place for responding to bomb threats, including gathering information from callers and handling suspicious packages. Many courts have specialized forms that should be completed if a threat is received. Court staff should be trained in how to record calls when received. Staff should be trained in recognizing potential indicators of a mailed threat, and mailrooms should implement screening procedures.



L. Mail

Procedures for screening and handling mail threats should be established, including reporting and preserving evidence. Staff should be trained to recognize potential indicators of mailed threats, such as suspicious packaging or unusual content.

M. Terrorism

Courts should develop plans in conjunction with security officers and law enforcement agencies to respond to terrorist incidents. Plans should focus on ensuring the safety of staff and visitors and restoring normal operations as quickly as possible.

N. Cyber Attacks

Over the past decade, the frequency and severity of cyber-attacks, malware infections and network hijackings have escalated. As courts embrace the digital age with computer systems, smartphones, and electronic devices, they face increased exposure to cyber threats. Cyber-attacks can cripple court operations, rendering networks and systems inoperable until a ransom is paid. The saying "It's not a matter of if, but when" underscores the inevitability of facing such attacks in today's digital landscape.



To counter these threats, courts must allocate resources to bolster their infrastructure and cybersecurity measures. Firewalls, antivirus software, and intrusion detection systems are essential tools to protect networks and computers from unauthorized access and malicious software. Comprehensive training programs for court staff are imperative to ensure adherence to safe internet practices and to recognize potential threats. Staff should be taught how

to identify phishing attempts, avoid clicking on suspicious links, and report any unusual activity promptly.

States increasingly incorporate cybersecurity training into their certification programs for court personnel. This training equips staff with the knowledge and skills needed to safeguard sensitive court data and systems from cyber threats. The training should be updated regularly to encompass ever-evolving threats.

In addition to preventive measures, courts should establish protocols for responding to cyber-attacks swiftly and effectively. This includes procedures for isolating infected systems, restoring data from backups, and coordinating with law enforcement agencies for investigation and prosecution of perpetrators.

Regular audits and assessments of court systems and networks are crucial to identify vulnerabilities and address potential risks proactively. By staying vigilant and proactive in their approach to cybersecurity, courts can mitigate the impact of cyber-attacks and safeguard the integrity of judicial proceedings.

Chapter 9: Conclusion

As we conclude this guide on court security for administrators in 2024, let us reflect on the importance of maintaining a proactive and adaptive approach to security management. In an era marked by dynamic threats and emerging



challenges, it is essential for court administrators to remain vigilant, informed, and prepared to address security concerns.

By understanding current threats, updating policies, leveraging technology advances, enhancing emergency preparedness, ensuring accessibility and inclusivity, engaging

stakeholders, and providing training resources, court administrators can promote a safe and secure environment for all stakeholders.

As we strive to uphold the principles of justice, fairness, and safety in our court systems, let us continue to collaborate, innovate, and adapt to meet the evolving security needs of our communities.

APPENDIX A

Areas of Concern in a Security Survey

Facilities

Exterior

- Perimeter (e.g., fences, gates)
- Lights
- Parking areas
- Access roads
- Landscaping

Building

- Doors, windows, other openings
- Ceilings, walls
- Interior lights (including switches and fuses)
- Emergency power system
- Alarm systems
- Safes and vaults
- Fire protection
- Utility control points
- Attics, basements, crawl spaces, air-conditioning and heating ducts
- Elevators, stairways
- Storage areas for arms and dangerous substances
- Communications areas
- Computer/Server room
- Records storage areas
- Conference rooms
- Offices handling money
- Food service areas
- Non-court offices
- Restrooms

Courtrooms and related areas

- Courtrooms
 - *Location*
 - *Doors, windows, other openings*
 - *Lights*
 - *Furnishings*
- Chambers and related offices

- Clerk of the court
- Witness waiting rooms
- Attorney-client conference rooms
- Jury deliberation rooms
- Grand jury room
- Prisoner reception area
- Restricted and secure passageways
- Temporary holding areas
- Security equipment storage areas

Procedural

- Emergency plans (fire, evacuation, bomb threat)
- Visitor control
 - Courthouse
 - Courtroom
- Separate circulation routes for prisoners, court staff and general public
- Alarm response
- General court security procedures
- Night court requirements
- Building security procedures
- Building fire and safety codes
- Key and lock control
- Employee security orientation and training
- Shipping, receiving, and trash disposal
- Cash transfer
- Package inspection
- Tenant activity requirements (hours, number of visitors, etc.)
- Exhibit security and disposal

Administrative/Personnel

- Employment process
- Contractual process
- Training
- Monitoring staff, accountability
- Computer access
- Building access

Appendix B

Courtroom or Courthouse Security Order

(CASE CITE)

ORDER RE: SECURITY

This court has received information from investigative and public sources that the potential exists for the disruption of orderly proceedings in this (case) (courthouse).

IT IS THE ORDER OF THIS COURT that the sheriff of (INSERT NAME OF COUNTY) shall initiate the following security measures immediately until rescinded by further order of this court, in and around designated security areas in the (INSERT LOCATION).

1. All persons entering the (courtroom) (courthouse) shall be searched for weapons including their person, briefcases, packages, and containers of all description. Failure to submit to search shall result in denial of entry into the (courtroom) (courthouse). Body searches may only be conducted by same-sex officers.
2. Bags, packages, or containers of unreasonable size shall be excluded from the (courtroom) (courthouse).
3. Cellular phones shall not be allowed in (courtroom) (courthouse).
4. All persons entering the (courtroom) (courthouse) during proceedings must show valid and satisfactory identification upon demand by the sheriff. Failure to produce identification upon demand will result in denial of entry into the courtroom.
5. The sheriff shall provide adequate personnel to ensure a proper level of security in the security areas.

DATED:

Judge

Appendix C

Instructions for Bailiffs Guarding Sequestered Jurors

(COURT CAPTION)

(CASE CITE)

INSTRUCTIONS FOR BAILIFFS GUARDING SEQUESTERED JURORS

Sequestration means keeping the jurors together in the charge of an officer of the court, so they are kept away from any sort of outside communication or influence. You, as a (County) deputy sheriff, are an officer of the court.

1) DO NOT ALLOW jurors to discuss the case amongst themselves or with anyone else, including you, before they retire to deliberate. If they do try to talk about the case, the crime, or the penalty, try to change the subject, or courteously remind them they cannot talk about it.

2) Jurors MUST follow the following rules:

a) Jurors MAY NOT have visitors.

b) Jurors MAY NOT read newspapers or magazines.

c) Jurors MAY NOT listen to the radio.

d) Jurors MAY NOT watch television.

e) Jurors MAY NOT discuss the case with anyone, you or amongst themselves.

* The court must pre-approve all reading materials including books and magazines.

3) Please keep the jurors in a group as much as possible.

a) If they have to be divided up, a bailiff MUST be with each group.

b) Keep the jurors close together at meals; all jurors do not have to sit at the same table.

c) Make certain the jurors are seated away from the public and that there are no magazines or newspapers or operating televisions and radios around. Make sure they DO NOT overhear other people, not on the jury, discussing the case.

4) YOU MAY take the jurors for a walk on the levee if they wish. If some of them want to stay in the jury room, a deputy MUST stay with them. A good time for walks is during extended recesses in the morning or afternoon.

- 5) IF ANY emergency or questions arise, call the JUDGE to make decision.
- 6) The van must stay with the jurors at all times.
- (*) The jurors may call after they have been selected as a juror, in order to make arrangements for clothing, personal belongings and family obligations. These telephone calls must be monitored to be certain discussion about the case does not occur.

THIS _____ DAY OF _____, 20_____.

JUDGE

(DATE)

BE IT KNOWN that the foregoing has been read and understood by the following deputies:

SIGN AND PRINT YOUR NAME

Appendix D

Bomb Threat Checklist

BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

• No return address	• Poorly handwritten
• Excessive postage	• Misspelled words
• Stains	• Incorrect titles
• Strange odor	• Foreign postage
• Strange sounds	• Restrictive notes
• Unexpected delivery	

** Refer to your local bomb threat emergency response plan for evacuation criteria*


DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- **911**
- Follow your local guidelines

For more information about this form contact the
Office for Bombing Prevention at: OBP@cisa.dhs.gov



BOMB THREAT CHECKLIST

DATE: _____

TIME: _____

TIME CALLER HUNG UP: _____

PHONE NUMBER WHERE CALL RECEIVED: _____

Ask Caller:

- Where is the bomb located?
(building, floor, room, etc.) _____
- When will it go off? _____
- What does it look like? _____
- What kind of bomb is it? _____
- What will make it explode? _____
- Did you place the bomb? Yes No _____
- Why? _____
- What is your name? _____

Exact Words of Threat:

Information About Caller:

- Where is the caller located?
(background/level of noise) _____
- Estimated age: _____
- Is voice familiar? If so, who does it sound like? _____
- Other points: _____

Caller's Voice	Background Sounds	Threat Language
<input type="checkbox"/> Female	<input type="checkbox"/> Animal noises	<input type="checkbox"/> Incoherent
<input type="checkbox"/> Male	<input type="checkbox"/> House noises	<input type="checkbox"/> Message read
<input type="checkbox"/> Accent	<input type="checkbox"/> Kitchen noises	<input type="checkbox"/> Taped message
<input type="checkbox"/> Angry	<input type="checkbox"/> Street noises	<input type="checkbox"/> Irrational
<input type="checkbox"/> Calm	<input type="checkbox"/> Booth	<input type="checkbox"/> Profane
<input type="checkbox"/> Clearing throat	<input type="checkbox"/> PA system	<input type="checkbox"/> Well-spoken
<input type="checkbox"/> Coughing	<input type="checkbox"/> Conversation	
<input type="checkbox"/> Cracking Voice	<input type="checkbox"/> Music	
<input type="checkbox"/> Crying	<input type="checkbox"/> Motor	
<input type="checkbox"/> Deep	<input type="checkbox"/> Clear	
<input type="checkbox"/> Deep breathing	<input type="checkbox"/> Static	
<input type="checkbox"/> Disguised	<input type="checkbox"/> Office machinery	
<input type="checkbox"/> Distinct	<input type="checkbox"/> Factory machinery	
<input type="checkbox"/> Excited	<input type="checkbox"/> Local	
<input type="checkbox"/> Laughter	<input type="checkbox"/> Long distance	
<input type="checkbox"/> Lisp		
<input type="checkbox"/> Loud		
<input type="checkbox"/> Nasal		
<input type="checkbox"/> Normal		
<input type="checkbox"/> Ragged		
<input type="checkbox"/> Rapid		
<input type="checkbox"/> Raspy		
<input type="checkbox"/> Slow		
<input type="checkbox"/> Stutter		
<input type="checkbox"/> Soft		

Other Information: _____

V2

Appendix E

Emergency Action Plan

EMERGENCY ACTION PLAN (TEMPLATE)

2022

EMERGENCY ACTION PLAN

Facility Name:

Facility Address:

Date prepared/reviewed:

EVACUATION ROUTES

Evacuation route maps have been posted in each work area.

The following information is marked on evacuation maps:

1. Emergency exits
2. Primary and secondary evacuation routes
3. Locations of fire extinguishers
4. Fire alarm pull stations' location
5. Assembly points

****Site personnel should know at least two evacuation routes.**

EMERGENCY PHONE NUMBERS

EMERGENCY CONTACT	PHONE NUMBER
Fire Department:	
Police:	
EMS/Ambulance:	
President Judge:	
District Court Administrator:	
AOPC Judicial Programs:	
Risk Manager:	
Facilities Manager:	
Property Owner:	
Other:	

UTILITY COMPANY EMERGENCY CONTACTS

(Specify name of the company, phone number and point of contact)

UTILITY COMPANY	PHONE NUMBER
Electric:	
Water:	
Gas (if applicable):	
Telephone:	
Other:	

EMERGENCY REPORTING AND EVACUATION PROCEDURES

Types of emergencies to be reported by site personnel are:

- Severe Weather
 - Fire/Explosion
 - Bomb Threat
- Suspicious Mail/Package
 - Active Attacker
- Medical Emergencies
 - Utility Outage
- HAZMAT (Hazardous materials)
 - Judicial Threat

SEVERE WEATHER

Severe weather refers to any dangerous meteorological phenomena with the potential to cause damage, serious social disruption, or loss of human life.

- Flood
- Severe Winter Storm
- Tornado
- Earthquake

PRE-EVENT ACTIVITIES:

- Have a plan for major weather emergencies including in part: flooding, tornados, protracted heat waves, snow/ice storms, earthquakes or hurricanes
 - Determine a safe place in the office if a shelter-in-place is required
- Identify persons with special medical needs in the emergency preparedness plan
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Determine how best to shelter in place or evacuate as many be required
 - Provide essential care for children, disabled or anyone injured
 - Notify local authorities if evacuation or sheltering in place is required
 - Do not risk injury or death trying to perform unsafe rescues
- During a violent storm, avoid windows, doors and even concrete which may conduct lightening
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Do not try to return to evacuated locations unless authorized by local authorities
- Advise court administration of property damage as may be warranted for the situation
 - Clear minor debris that might impede first responders and utility workers
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

FIRE/EXPLOSION

A rapid conflagration or explosive detonation in which substances combine chemically with oxygen from the air and give out bright light, heat, smoke and energy.

- Combustible fires
 - Chemical fires
 - Electrical fires
- Explosive detonations

PRE-EVENT ACTIVITIES:

- Develop a plan to survive; educate to evacuate
- Verify the adequacy and operability of smoke detectors and fire extinguishers
 - Identify several exits for potential emergency evacuation
 - Ensure critical documents are stored in a fire proof safe
 - Practice fire drills
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Verify everyone is out of the building
- Call '911' and advise if anyone is unaccounted
- Use fire extinguishers to aid in the evacuation
- Close doors upon exiting; air fuels the fire
- Secure critical documents while exiting
- Evacuate; crawl out if smoke is present
- Assist those with injuries or disabilities
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Render or seek first aid for injuries
- Notify court administration as may be appropriate
- Law enforcement and AOPC Communications will coordinate public statements
- Never re-enter a burned structure without fire department/municipal authorization
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

BOMB THREAT

A bomb threat is a threat, usually verbal or written, to detonate an explosive device to cause property damage, death, injuries and/or excite fear, whether or not such a device actually exists.

- Telephone bomb threat
- USPS written bomb threats
- Emailed or texted bomb threats
- Social media bomb threats
- ADD CONTENT AS APPLICABLE
- ADD CONTENT AS APPLICABLE

PRE-EVENT ACTIVITIES:

- Be prepared to act decisively if a bomb threat is received
- Be sure all staff know what to do if a bomb threat is received at the court
- Ensure emergency procedures are clearly understood by all stakeholders
 - Keep “bomb threat checklists’ near all telephones
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- If a telephone bomb threat, listen carefully and document exact words, background noises and vocal characteristics
 - Copy caller’s telephone number if displayed
 - Complete a bomb threat checklist
- Evacuate, if directed by law enforcement, to a safe location well-away from the building or unknown vehicles
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Law enforcement and AOPC Communications will coordinate public statements
 - Relinquish any evidence to law enforcement
 - Ensure all areas searched are re-secured/locked
- Cooperate with law enforcement; a suspect is often identified
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

SUSPICIOUS MAIL/PACKAGES

Suspicious packages include any package that is unexpectedly delivered or deposited and exhibits unusual characteristics.

- Unexpected arrival
- Restricted to addressee
 - Atypical location
 - Excessive postage
- Sender information absent

PRE-EVENT ACTIVITIES:

- Be prepared to act decisively if a suspicious package is received or discovered
- Be sure all staff know what to do if a suspicious package is received at the court
- Determine a rally point far removed from the court if an evacuation were to be ordered
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Call '911' if a suspicious object is located at a court facility
- Stay away from the object until deemed safe by law enforcement
- If opened, wash your hands with soap and water for at least two minutes; disrobe clothing that was exposed to any contaminants
- Advise President Judge and District Court Administrator of the event
 - Do not handle the envelope/parcel after deeming it suspicious
- Evacuate, if directed by law enforcement, to a safe location away from the building or parcel
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Law enforcement and AOPC Communications will coordinate public statements
 - Seek medical evaluation if suspicious powders or liquids are discovered in envelope/package
- Cooperate with law enforcement's efforts to identify the sender if the parcel is deemed suspicious and unwanted
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTIVE SHOOTER

An active attacker is defined as an individual actively engaged in killing or attempting to kill people in a confined and populated area.

- Have a plan
- Run, Hide, Fight
- Shelter in place if necessary
 - Fight to survive

PRE-EVENT ACTIVITIES:

- Be prepared to act quickly in an active attacker situation; mere seconds are pivotal in avoiding or sustaining injuries
- Remain alert at all times to the potential that an emergent situation might erupt in a court facility
 - Memorize 'Run, Hide, Fight' and know what action may be require in an emergency
 - Partner with law enforcement for best practices and training
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- If you can run, abandon personal items and flee the scene quickly and quietly; flee far and hide
- If you must hide, shelter in place quickly and quietly to thwart an attacker gaining access to your location
- If you must fight, attack violently and thoroughly incapacitate the attacker; then run for safety
 - Call '911' when it is safe to do; act first, then call!
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Do not expose yourself to unnecessary danger by attempting to aid the wounded; first aid should commence only after the situation is deemed safe
 - Render first aid/stop the bleed as necessary
- Keeps hands visible and follow police commands when they arrive; provide suspect(s) description if noted
 - Law enforcement and AOPC Communications will coordinate public statements
 - ADD CONTENT AS APPLICABLE

MEDICAL EMERGENCIES

Medical emergencies involve acute sudden illness or traumatic injuries.

- Medical
 - Call '911'
 - CPR/AED
 - First Aid
 - Stop the Bleed
- Blood borne pathogens

PRE-EVENT ACTIVITIES:

- Plan to react to medical emergencies at court; calling '911' is just a start
 - Participate in a First Aid/CPR/AED and Stop the Bleed training courses
- Ensure that a well-stocked first aid kit, equipped with tourniquets and hemostatic bandages is accessible
- Ensure an adequate supply of personal protective equipment (PPE) is available to provide body substance isolation (BSI)
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Think safety first; ensure scene safety before taking action
- Call '911' and inform dispatchers of the location, nature of the medical emergency and what is being done to aid those involved. Don't hang up the phone, dispatchers may need to provide instructions
- Provide first aid consistent with training, if necessary, or endeavor to provide emotional support until first responders arrive
- Tell first responders what happened and what was done for the patient upon their arrival
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Advise court administration of medical emergencies occurring in the court facilities
 - Document the event in detail; witness information should be included
 - Dispose of PPE properly; use hand sanitizer
 - Ensure the scene is professionally cleaned
 - Refer medical reporters to police for information

- Consider critical incident stress debriefing or employee assistance program counselor services as may be necessary

UTILITY OUTAGE

Utility outages refers to any protracted unavailability of public utilities that may cause serious social disruption, including:

- Electrical power outage
 - Gas line rupture
- Contaminated water supply
 - Public sewer dysfunction
- Cable/telecommunications failure

PRE-EVENT ACTIVITIES:

- Determine emergency notification numbers for all utility providers
- Be aware of utility shutoffs, electrical meters and electrical panel boxes
- Consider back-up power resources like outdoor emergency generators
- Be aware that both landline and cellular phone systems may be unavailable
- Stay informed to get vital emergency updates; a battery powered radio is a must
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Notify the public utility promptly if services are lost
- If directed by the President Judge, close the court facility if there is a loss of public utilities like water, sewer, electricity, telecommunications, cable or natural gas
- Disconnect electronics and computers in the event of power surges upon the resumption of power
 - Keep refrigerator and freezer doors closed to preserve coldness
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Check all building systems for operability when power resumes
- If the power outage is a result of a major storm, check for property damage; avoid downed wires and trees

- Notify court administration and insurance carriers of damage
- Verify time correctness on computers, remote devices and clocks
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

HAZMAT EVENT

HazMat/Hazardous Materials Emergency refers to any emergent public health risk caused by a release of a hazardous chemical, biological, or radiological material.

- Chemical truck crash
- Freight train derailment
 - Industrial fire
- Radiological waste spill

PRE-EVENT ACTIVITIES:

- Identify various situations that might result in a local HazMat event
- Determine best practices for sheltering in place or evacuating if required
 - Determine how to turn off HVAC (ventilation systems)
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- Act quickly if you have come into contact with or have been exposed to hazardous chemicals
 - Follow decontamination instructions from local authorities
 - Seek medical treatment for unusual symptoms as soon as possible
 - Place exposed clothing and shoes in tightly sealed containers
- Advise everyone who comes into contact with you that you may have been exposed to a toxic substance
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Verify the scene's safety and security with first responders before entering the court facility
 - Schedule special cleaning if warranted

- Report any lingering vapors or other hazards to your local emergency services office
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

JUDICIAL THREAT

Judicial Threats refers to any direct (Explicit) or indirect (implicit) threat made towards a judge, including:

- Written threats
- Telephone threats
- Social media threats
 - E-mail threats
- Third party communications
- Symbolic Vandalism

PRE-EVENT ACTIVITIES:

- Be prepared to act decisively if a judicial threat is received
- Be sure all staff know what to do if a judicial threat is received
- Ensure emergency procedures are clearly understood by all stakeholders
 - Keep emergency contact lists near all telephones
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

ACTUALIZED EVENT ACTIVITIES:

- If a threat is conveyed by any means, document all persons involved and the exact words used
 - Minimize handling of handwritten correspondence
- Advise local police, sheriff, president judge, and district court administrator of the event
- Apprise AOPC/Judicial District Security that a threat has been received and what was communicated; File a PAJIRS report promptly
 - If conveyed by telephone, copy caller's telephone number if displayed
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

POST EVENT ACTIVITIES:

- Law enforcement and AOPC Communications will coordinate public statements
 - Relinquish any evidence and CCTV images to law enforcement
 - Initiate a PAJIRS report as soon as practical
 - Endeavor to obtain a photograph of the subject
 - If the actor is arrested, request notification of their release from prison
 - Exercise enhanced vigilance at court, in transit and while at home
- Ensure all security measures and technologies are functioning as intended
 - ADD CONTENT AS APPLICABLE
 - ADD CONTENT AS APPLICABLE

Appendix F

The Pennsylvania Judicial Incident Reporting System (PAJIRS)

The PA JUDICIAL INCIDENT REPORTING SYSTEM (PAJIRS) is a proprietary web-based incident reporting program that provides judges, district court administrators, judicial staff, and county sheriffs with the ability to electronically submit security-related incident reports as required by Pennsylvania Rule of Judicial Administration 1954(B).

PAJIRS incident reports to AOPC's Office of Judicial District Security are promptly reviewed and the information is confidentially managed. Based on the nature of the situation being reported, security guidance is provided to the reporting parties to further ensure effective risk mitigation. PAJIRS data is also analyzed to identify trends in incident activity, frequency of occurrence, and location of events. This information is further considered by the Commonwealth's legislature in their annual appropriation of security grant funding and by the Office of Judicial District Security during security project planning for judicial districts.

Reportable incidents include:

1. Attempted or actual acts of violence or vandalism to persons or property of the court.
 - A defendant in a criminal proceeding attempts to attack the judge.
 - The court is vandalized with spray paint.
2. Any verbal or written threats portending actual or potential violence or harm.
 - A litigant posted on social media a picture of the judge's family with intent to harm them.
 - A litigant writes a letter threatening violence if the judge does not rule in their favor.
3. Any police/fire/EMS dispatch or response.
 - Smoke suddenly fills the court.
 - A litigant has an apparent heart attack.
4. Any weapons brandished, or menacing behaviors exhibited.
 - A litigant aggressively displays his fists upon entering the court.
 - A litigant exits the court, gets a baseball bat out of his car, and aggressively walks back toward the court.
5. Suspicious packages discovered, or bomb threats received.
 - An unknown package is discovered at the front doors of an MDJ Office.

- An unidentified caller states a bomb has been placed in the courthouse.

6. Any prohibited offensive weapons or contraband detected.

- Brass knuckles are detected in a litigant's personal effects.
- Several packets of suspected drugs are located in the restroom.



National Association
for **Court Management**

National Association for Court Management
300 Newport Avenue
Williamsburg, VA 23185-4147
Phone (800) 616-6165