STEPS TO BEST PRACTICES *for* COURT BUILDING SECURITY

Revised June 2022

National Center for State Courts

ACKNOWLEDGEMENTS

The development and publication of this revised report has been made possible by the support and hard work of many people. The National Center for State Courts (NCSC) wishes to acknowledge the following individuals who have worked to developed and revise this document over the years: Nathan Hall, Principal Court Management Consultant at the NCSC and security consultants Steven Berson, Timothy Fautsko, James O'Neil, Kevin Sheehan, Justin Mammen and Judge Lee Sinclair. The NCSC also extends its appreciation to the members of the Conference of Chief Justices/Conference of State Court Administrators Security and Emergency Preparedness Committee and their staffs for carefully reviewing this document and making important recommendations that have improved the final product. Finally, the NCSC extends thanks to its editorial staff over the years, for the many hours they spent providing quality assurance in the conformation and final editing of the original and revised publications.

Published February 2010.
Revised January 2013.
Revised September 2016.
Revised June 2022.

TABLE OF CONTENTS

INTRODUCTION

The National Center for State Courts (NCSC), through its Court Consulting Services division, has conducted security assessments of court buildings as well as personal security and safety training throughout the country. In conducting court building assessments, the NCSC has evaluated court security in terms of "best practices" – guidelines describing those security measures that should be in place concerning a comprehensive set of topics on court buildings and court operations. These best practices are not only based on the considerable experience of NCSC security experts, but are also consistent with guidelines from the United States Marshals Service, National Sheriffs' Association, Conference of Chief Justices/Conference of State Court Administrators Joint Committee on Court Security and Emergency Preparedness, International Association of Chiefs of Police, Transportation Safety Administration, the Department of Homeland Security, and the National Association for Court Management. The NCSC recommends that leadership in every court building strive to achieve best practices in all topic areas to provide a suitable level of security for all those who work in or visit the court building.

Implementing some of the best practices in court building security may be a challenge to constrained or limited budgetary resources. Accordingly, best practices are set forth in a format of steps and phases as an incremental approach that envisions an effective level of security upon implementation of all measures. These steps may be a useful approach to courts as they strive to implement improvements in court building security. The NCSC wishes to emphasize that an effective level of security will be reached when all the measures at the best practices level are incorporated. The NCSC has provided these steps in phases, so that a court may use its discretion to incrementally adopt improvements before reaching the level of best practices. These steps and phases are laid out as plateaus along an ascending path to improvement – improvement the NCSC recommends that courts achieve over time.

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

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

TERMS USED IN STEPS TO BEST PACTICES

- Steps: These are specific buildings blocks and/or specific actions that courts can take to improve security.

- Phases: These are logical groupings of steps forming a temporary plateau in terms of security measures in place.
- Topics: These are the subject areas into which steps in phases are organized.
- Categories: These are sets of topics. There are three categories listed in priority order, with Category A taking top priority.
    - Category A: These are fundamental topics that should be addressed first in order to provide a base on which to place all of the other topics.
    - Category B: These are critical topics to be addressed after the Category A topics.
    - Category C: These are essential topics to be addressed after the Category A and B topics.

CATEGORY A: FUNDAMENTAL

The following four topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices for Court Building Security*. The recommended measures in Category A are those that typically can be implemented with relatively limited cost. For example, operating a security committee or developing and implementing policies and procedures may incur time and effort on the part of staff but do not, as a rule, involve or cause additional expenditures from court budgets for such "hard-cost" items like equipment or facilities improvements.

- **A-1: Security Committee.** A court building security committee that meets regularly and is empowered to exercise oversight and sustain matters related to security within the court building is a prerequisite to enable the court and its stakeholders to properly assess and address the myriad security challenges facing court and stakeholder leadership.

- **A-2: Policies and Procedures.** A cohesive and comprehensive set of security policies and procedures is necessary to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices for Court Building Security* to further the process of developing a meaningful and effective set of policies and procedures.

- **A-3: Threat and Incident Reporting.** Threat and incident reporting is of paramount importance to the safety of judges, court employees, and the public who visit the court building. Enacting a threat and incident reporting system enables stakeholders to review and develop responses to potential negative events and reinforces security best practices.

- **A-4: Security Training.** Every single person who works in a court building has the potential to materially enhance the safety and security of his or her work environment, to be the "eyes and ears" of a workforce constantly alert to risks and threats. Judges and court staff that have been well-trained on well-publicized policies and procedures provide the best eyes-and-ears function.. Moreover, a cadre of well-trained Court Security Officers are a necessity for a safe and secure court building.

TOPIC A-1: SECURITY COMMITTEE

PHASE ONE

1. Establish a court building security committee for the court building, to be chaired by a judge (preferably presiding) and having membership of at least the primary security provider and a representative of the county or other funding source. The committee should serve as the primary champion for attainment of the best practices outlined in this document and should, in particular, assume as one of its primary responsibilities the achievement of the foundational elements set forth in Topics A-1 thru A-4.
2. The court building security committee should operate its meetings on an action-planning process of "who does what, by when, and what resources are needed." The committee should initially meet monthly to identify and discuss security challenges facing the court building, and devise and implement solutions to meet those challenges. Then, it should meet at least quarterly to discuss security problems and track progress on an ongoing basis.
3. The presiding judge or court administrator, as representatives of the court building security committee, should meet with court security personnel and law enforcement officials on a regular basis and after any negative event to discuss security concerns and improve security at the court building.

PHASE TWO

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

4. Add security committee members representing all "stakeholders" who have an interest in security at the court building. Stakeholders, by way of example, include county facilities management, the district attorney and public defender, the state or local bar, the probation department, and other non-court tenants of the court building. In terms of the size of the committee, a balance should be struck between ensuring stakeholder inclusivity and the need to keep the committee at a manageable size. (Stakeholders not represented on the committee can be appointed to tasks forces per Step 6 below.)

PHASE THREE

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

5. Undertake an assessment of the security in place within the court building. Assistance in conducting assessments is available from the NCSC.

BEST PRACTICE

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

6. As needed, and under the auspices of the security committee, form task forces to provide the committee with additional research and information gathering capacity.[1] Additional members added to various task forces could include:
    - Court staff members working in the court building, to include appropriate staff with expertise and responsibility related to the issue to be addressed by the task force
    - Judicial stakeholders, including local and state government and law enforcement officials
    - Local and state subject matter experts
7. One or more members of the court building security committee should actively participate in any committee or working group established for court facility design, construction, and renovation projects.
8. Periodically engage an independent professional organization to conduct an audit of security measures in place for the exterior and interior of the court building.

TOPIC A-2: POLICIES AND PROCEDURES

PHASE ONE

1. Under the auspices of the court building security committee (see Topic A-1), the leadership of the court, county (or other funding body), and law enforcement should understand the need for and commit to the development and implementation of effective and comprehensive court building security policies and procedures. It is important to note that it is particularly crucial for judges to be at the forefront of court building security, providing leadership in the development and implementation of security policies and procedures.
2. Under the auspices of the court building security committee, and with the cooperation of the appropriate law enforcement agency(s), develop a cohesive and comprehensive set

[1] For example, an "Incident Reporting and Threat Assessment" task force could be chaired by a member of the security committee and oversee implementation of an incident reporting and threat assessment system that not only collects data, but actively analyzes it, reports on actions taken, and presents recommendations for change to the committee.

of court building security materials, to include such items as policies and procedures, operations manuals, training manuals, contingency plans, and incident reporting and risk assessment instruments and protocol. NOTE: Policies and procedures should be developed to include the topics listed in Appendix A.

PHASE TWO

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

3. Establish communication protocols with court staff and stakeholders that allow for feedback and revision of security materials as follows:
    - Provide periodic briefings in various formats to court staff and stakeholders.
    - Solicit formal feedback from court staff and stakeholders.
    - Revise court building security materials as necessary based on court staff and stakeholder feedback.
4. Officially adopt the court building security materials and issue appropriate court orders on key security matters. To be successful, security documents need the support of judicial leadership. Court orders give legitimacy and enforceability to security policies.
5. Publish the court building security materials. The level of detail and the audience to whom materials are published should be determined on a need-to-know basis.

PHASE THREE

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

6. Practice and evaluate the court building security materials as follows:
    - Conduct drills and exercises to test policies and procedures.
    - Evaluate the results of the drills.
    - Evaluate the results of responses to actual negative events and incidents.
    - Revise the court building security materials as warranted based on an evaluation of the results of drills and actual incidents.
7. Invite first responders including SWAT units to walk the court building and grounds to familiarize the first responders with the facilities. Request that the SWAT unit utilize the court building for training on a periodic basis.

BEST PRACTICE

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

8. Review and update policies and procedures on at least a biennial basis and after major incidents, events, and facility renovation projects.

9. Analyze the activities undertaken in Phases Two, Three, and Four for operational effectiveness.

TOPIC A-3: THREAT AND INCIDENT REPORTING

DEFINITIONS

THREAT – is a statement or behavior that signals an intention to inflict pain, injury, damage, or other hostile action on someone (court employee or court attendee) or an institution (court building) in retribution for something done or not done now or in the future. A threat is synonymous with a threatening remark, behavior, warning, or ultimatum to a person or institution. A threat can be a person or a thing likely to cause damage or danger.

INCIDENT – is an action or communication that causes or threatens to cause personal injury, property damage, or disrupts court building proceedings. Court building proceedings include activities in the courtroom and outside the courtroom and within the facility (e.g., chambers, clerk's offices, etc.). NOTE: This definition is focused on the potential that an action may manifest physically (personal injury, property damage) or be a threat of the same.

PHASE ONE

1. Establish a policy requiring threats and incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible, but no later than the close of business on the day in which a threat or incident occurred. The more serious the threat or incident, the more quickly it should be reported.
2. Coordinate with law enforcement to ensure that all threats and incidents are thoroughly assessed and that appropriate responses and/or mitigation steps are taken.
3. Train Court Security Officers[2] (CSOs), judges, and staff in the court building on how to recognize threats and incidents and how to report them orally and in writing.
4. Develop and use threat and incident reporting forms and submit forms in writing to the proper authorities, at least monthly, preferably in electronic format so the designated reporters can more easily file their reports and necessary guidance/assistance can be

[2] COURT SECURITY OFFICER (CSO) – A Court Security Officer (CSO), as referenced throughout this document, is defined as an individual trained and qualified in court building security, and has been specifically trained and qualified to use a firearm and intermediate weapons such as Taser, chemical spray, or restraints (e.g.,. handcuffs, leg restraints). A summary of CSO staffing recommendations included in this document can be found in Appendix B.

provided more readily. The court building security committee should receive a copy of all threat and incident reports.

5. Coordinate threat and incident information with interested parties at the state and local level.

PHASE TWO

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

6. Implement a practice for regularly evaluating threat and incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court building security committee (and the committee's incident reporting task force).
7. Provide feedback to staff on threats and incidents, particularly to those who reported them (i.e., complete the feedback loop).

BEST PRACTICE

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

8. Establish threat and incident information sharing with state or metropolitan fusion centers.[3]
9. Train CSOs or appropriate staff on how to monitor social media platforms to identify and track potential threats. If trained staff are not available, consider seeking assistance from a fusion center or local law enforcement agency.
10. Establish an electronic system for reporting threats and incidents to enable quick review and deployment of resources and to enable organization of data and analysis by law enforcement and authorized stakeholders. A database should be maintained on all pertinent information, to include organizational responses and any follow-up activities. Databases should be maintained at the local and state level.

[3] According to the Department of Homeland Security, fusion centers are state-owned and -operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial (SLTT); federal; and private sector partners. For more information, see the Department of Homeland Security Website at: https://www.dhs.gov/fusion-centers.

TOPIC A-4: SECURITY TRAINING

NOTE: Training is the glue that binds all court building security measures together. Security training needs to be frequent, repetitive, and simple. Without training, staff and CSOs will never be prepared for the unexpected. Every staff member and CSO needs security training. It is essential that training be mandatory and universal. Judges in particular need to participate. Nothing gets staff to buy in to security more than a judge actively participating in security training. The judge sets the tone.

PHASE ONE

1. New judges and court staff should receive an initial court security orientation briefing that includes such topics as shooter in place and hostage-taking, emergency procedures (e.g., for fire, weather, and medical emergencies), building evacuation routes, and personal safety procedures for work and home.
2. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.
3. CSOs should be trained in basic court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, threat de-escalation techniques, and safety and weapons certification**.**
4. CSOs should receive basic training in emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage situations, active-shooters, and judicial protection.
5. Command center staff should be trained in critical incident command and crisis communications. Communication during an emergency must be clear, understandable, and simple.

PHASE TWO

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

6. Establish a judge and staff security continuing education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and off-site.
7. Invite first responders, particularly the SWAT team, to do a walk-through of the court building. Encourage the SWAT team to utilize the court building as part of their own training program.

PHASE THREE

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

8. Establish mandatory, ongoing security and safety education programs for judges and court staff that include topics addressed in the initial security orientation briefing, along with such topics as handling difficult people, anger-management, home safety techniques, safety practices for inside and outside the court building, hostage incidents, and emergency evacuation from the court building.
9. In addition to annual familiarization and qualification courses on firearms and intermediate weapons, establish regularly scheduled mandatory advanced refresher training courses for CSOs, to include such topics as emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage situations, active-shooters, and judicial protection.

BEST PRACTICE

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

10. Establish mandatory ongoing security and safety education programs for judges and court staff that include high-profile trials, home safety techniques, travel safety tips, suspicious packages, bomb and other threats, and emergency evacuation from the court building. Train judges and court staff on self-defense options, threat de-escalation techniques, and personal safety/security considerations during hostage situations.
11. Establish and schedule advanced court security training programs for CSOs to include topics such as threat de-escalation, security assessments, judicial protection, security for domestic violence cases, incident response, dangerous individuals, mental health issues, and high threat proceedings. All CSOs should receive at least 24 hours of mandatory in-service training on court security each year.

CATEGORY B: CRITICAL

TOPIC B-1: COMMAND CENTER

NOTE: A security command center, as referenced in this document, refers to a physical location where all security activities for the court building are controlled and all security infrastructure is monitored. A security "command center" has a different function than an in-custody defendant "control room", which is used to manage the transport and housing of in-custody defendants. In some court buildings, the command center and control room are combined into a single facility to gain building and staffing efficiencies.

PHASE ONE

1. Until a proper dedicated command center can be established, install a security desk or workstation near the front entrance screening station to serve as the central location for control and monitoring of security systems.
2. Dedicate at least one full-time CSO position the staff the security desk (where resources are limited, this may be the same person who is assigned to secure the main public entrance to the court building as described in Topic B-6, Phase One).
3. Constantly monitor duress alarms[4] and security cameras[5] at the command center.
4. Provide alarm panels or posted diagrams at the command center that clearly and logically number each room in the court building to aid in response.
5. Establish telephone/radio communication points between the security desk and potentially vulnerable areas of the court building, such as courtrooms and chambers.
6. Establish telephone/radio communication between the security desk and local law enforcement, and/or emergency dispatch entities.

PHASE TWO

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

7. Construct a dedicated command center within the court building. Make sure that access to the command center is carefully restricted.
8. Assign a CSO to the dedicated command center. The assigned command center CSO is not necessarily required to carry a firearm.

[4] A summary of duress alarm recommendations included in this document can be found in Appendix C.

[5] A summary of cameras recommendations included in this document can be found in Appendix D.

9. Install control panels and monitoring equipment for security surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch. As noted above, all control panels should clearly identify locations in the court building to include rooms clearly and logically numbered to aid in emergency response.
10. Command center staff should have access to mass notification systems (e.g., public address systems, telephone notification systems, email, text, social media, etc.) installed in the court building to be able to communicate with building occupants in the event of emergencies. Staff should receive ongoing training on mass notification protocols and procedures (see related recommendation in Topic C-1, Step 9).
11. The individuals staffing the command center should not be the physical responders to a crisis. Removing them from the command center to be physically present at the scene of the crisis could result in the loss of a critical element providing situational awareness to emergency responders and staff. The situational awareness provided by the command center allows responders to make the best tactical decisions and staff to decide whether to shelter in place or run.
12. The command center should be staffed at all times when the court building is open the public.

BEST PRACTICE

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

13. Cameras should be integrated with duress and access control (door) alarms. When a duress or access control alarm activates, an image on the appropriate camera should activate on a monitor in the command center. The command center staff should not only have the ability to view the monitor but also to communicate via audio with staff activating the alarm.
14. Provide additional monitoring capacity for critical court building infrastructure including elevators, mechanical systems, emergency generators/generator fuel levels.
15. Provide additional security personnel as required to supervise and monitor command center activities.
16. In court buildings where the command center is situated in a vulnerable area (e.g., in the main entrance/lobby area with windows facing the exterior) and as justified by a threat assessment, provide ballistic-resistant protection over the command center's doors, windows, and other areas subject to attack.
17. After-hours monitoring of intrusion alarms and cameras should be provided. This may be accomplished through network linkage and coordination with local law enforcement, and/or emergency dispatch entities.

TOPIC B-2: IN-CUSTODY DEFENDANTS

PHASE ONE

1. Assign at least one CSO or transport deputy to escort in-custody defendants through all non-secure areas of the court building and to clear the path ahead of members of the public.
2. Assign one CSO to remain with in-custody defendants in the courtroom at all times.
3. In court buildings lacking secure in-custody defendant circulation zones (see discussion of circulation zones in Topic B-7), efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of members of the public is at a minimum. Ideally all members of the public should be moved to the far end of the hallway. If this is not possible, at least move members of the public to the side of the hallway prior to the escort of in-custody defendants.
4. When escorting in-custody defendants in a public elevator, the elevator should first be cleared of all members of the public.
5. In-custody defendants should be properly restrained while being escorted, using handcuffs, ankle restraints, and belly chains. (They should not be handcuffed from the front.)
6. In-custody defendants should have no contact of any type -- physical or verbal – with the public, family, or friends while being escorted or while in court.
7. Always check for holds and live warrants before releasing an in-custody defendant as a result of a courtroom proceeding.

PHASE TWO

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

8. Establish one or more dedicated holding cells where in-custody defendants may be held while waiting for their court hearing.
9. Make sure all holding cells within the court building are appropriately secured, staffed, and searched before and after each occupation.
10. Provide sight and sound separation, as required or appropriate, of different in-custody populations within secure in-custody holding and transportation areas (e.g., male, female, and juveniles). The design of these areas should prohibit unauthorized access by the public and escape by in-custody defendants.
11. Install security cameras (with tamper-resistant housings) in holding cells.
12. Install security cameras along the entire in-custody defendants' escort route including staging areas, hallways, and elevators.

13. Install duress alarms in circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators).
14. Establish a secure sally port for in-custody defendants entering the court building. The sally port should be equipped with a security camera and duress alarm (see also Topic B-9 for camera coverage of exterior areas leading to the sally port).
15. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the in-custody defendant should be armed with an intermediate weapon(e.g., Taser or chemical spray) and the other officer trailing behind should be armed with a firearm using a triple retention holster.
16. Provide remote video and audio linkages (and supporting infrastructure) to allow for reliable connectivity between the court and the detention centers for both adult and juvenile populations. Alternatively, establish a courtroom in the detention center(s) for advisements/arraignments and other hearings. From a security perspective, either measure minimizes the number of in-custody defendants brought into the courthouse and is a preferred solution to bringing in-custody defendants back and forth to the court buildings, particularly for arraignment settings and non-evidentiary hearings.

NOTE: The presence of in-custody defendants poses inherent security risks for those who work in and visit court buildings. During the COVID 19 Pandemic many state courts took steps to reduce and minimize the number of in-custody defendants brought into court buildings on a regular basis. These steps included:

- Providing technology tools connecting courtrooms remotely to detention centers and jails (for both adult and juvenile populations) to minimize the number of in-custody defendants brought into the court building.
- Providing suitable and adequate space to efficiently conduct remote proceedings at detention centers and jails.
- Limiting the number of transportation events to necessary in-court hearings for individuals in custody or receiving services pursuant to court order, including combining hearings (subject to maximum gathering size and to minimize the mixing of populations to eliminate avoidable quarantines when such individuals are returned to custody following court hearings).

Continuing to implement such steps, even in the aftermath of the Pandemic, will have a beneficial impact on the safety and security of court buildings.

BEST PRACTICE

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

17. Establish a control room to manage the transport and housing of in-custody defendants. The control center should include monitoring capacity and control of all doors, elevators,

cameras, and alarms within the secure in-custody defendant circulation area. As stated in Topic B-1, in some court buildings, this function may be located and managed together with the building security command center.

18. The control room should be staffed at all times when in-custody defendants are present in the court building.
19. Establish and maintain complete separation between areas used for the transportation of in-custody defendants and all other areas of the court building. This includes secure circulation for a defendant from the transport vehicle, through the sally port, through secure elevators, to the holding cell, and to the courtroom to avoid crossing the path of judges, jurors, staff, or the public.

TOPIC B-3: COURTROOMS

PHASE ONE

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a "rover" from one courtroom to the next (unless local or state rules require additional coverage).
2. There must be at least one CSO present throughout the entire court proceeding whenever an in-custody defendant is involved.
3. Install duress alarms[6] in the courtroom at accessible locations:
    - On top of or under the working surface of the bench, plainly marked
    - At the clerk's station
4. Train judges and staff on the functionality of duress alarms and on the protocols for use.
5. Test duress alarms regularly (at least monthly).
6. Courtrooms should be cleared and locked during a recess or when the courtroom is otherwise not in use. It should be possible to easily lock all courtroom doors from the inside. If individuals are allowed to stay in the courtroom during a recess, a CSO should be assigned to remain in the courtroom.
7. Secure or remove items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, water glasses). As substitutes for these items, use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers. There should be no drawers in plaintiff's or defendant's tables. Secure

[6] See Appendix C for a summary of information pertaining to duress alarms.

or remove all moveable furniture. (Moveable or folding chairs can be secured by fastening them together with secure ties around their legs.)

8. Install and then regularly test emergency lighting/fire equipment in courtrooms.
9. Use proper and acceptable restraints per state law and a judge's approval on in-custody defendants. In-custody defendants, except during a jury trial or as prohibited by law, should be restrained with handcuffs, leg restraints, and belly chains.
10. Install door scopes (i.e., peepholes) for the judge's entry into the courtroom.
11. Ensure weapons allowed in the courtroom as exhibits are rendered inoperable. Ammunition should always be secured in sealed evidence bags separate from any firearms. All evidence that has been admitted must be stored in a secured location to prevent tampering or theft when the court is recessed or not in session.
12. Judges presiding over courtroom matters should issue orders of decorum at the outset of all proceedings and should maintain vigilance in observing activities and maintaining decorum within the courtroom all times.
13. Judges, CSOs and court staff should maintain continual verbal and non-verbal communication regarding courtroom decorum and possible security issues throughout all court proceedings.
14. For high-visibility trials and for other proceedings as warranted, institute other security measures such as leaving the front row of the public gallery vacant and/or keeping separate family and friends of the plaintiff or prosecution from family and friends of the defendant.
15. Develop policies and procedures to keep defendants seated during pleas and sentencing hearings. A seated defendant is more easily controlled and less likely to be disruptive.
16. Keep presentation tables and podiums a safe distance away from the bench.
17. Conduct sweeps of all courtrooms. Sweeps should be made each time before the courtroom is opened and at the end of the day. If CSOs are not available, court staff can be trained and instructed to conduct courtroom sweeps. Logs must be made of sweeps to include descriptions of any items found during sweeps.

PHASE TWO

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

18. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in the courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present. The transport officer maintaining custody (i.e., having direct contact) of the in-custody defendant should be armed with an intermediate weapon (e.g., Taser, stun gun, or chemical spray, etc.) in lieu

of a firearm. This will minimize the likelihood of an in-custody defendant obtaining a firearm during confrontations.

19. CSOs in courtrooms should remain standing throughout the proceeding and positioned to be able to observe and to respond quickly to potential security incidents.
20. CSOs in courtrooms should manually lock down front door(s) in case of a security incident in the public area outside the courtroom.
21. Install at least one security camera in every courtroom. The primary security camera should be installed on the wall behind the bench facing the litigation area and public seating (refer to Best Practice level in this Topic for installation of an additional camera).
22. Establish separate entrance approaches and appropriate access controls into courtrooms for judges and court staff, jurors, in-custody defendants. Attorneys, witnesses, and the general public should enter courtrooms only through the main public entrance doors.
23. The courtroom door nearest the bench should allow the judge to quickly leave the courtroom in case of an emergency or security event and should lock behind the judge to thwart the pursuit by a potential assailant. If the door is required for public exit in the event of an emergency, a delayed egress device should be installed in accordance with local building codes.
24. Provide holding cells adjacent to courtrooms where matters involving the presence of in-custody defendants are regularly scheduled. Holding cells for the courtroom should be properly constructed, safe for the in-custody defendants, and escape-proof.
25. Install bullet-resistant materials at the bench and workstations inside courtrooms. Opaque ballistic-resistant material that meets UL Standard 752, Level III, should be installed behind the vertical surfaces on the three sides of the benches and stations that are visible to the public. Bullet-resistant fiberglass panels are a cost-effective material that can be field cut or factory cut to specific dimensions and installed on the backside of existing courtroom millwork. NOTE: The installation of bullet resistant materials should be highly prioritized if there is no weapons screening at the court building or if screening is materially deficient.

PHASE THREE

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

26. A second CSO should be assigned in the courtroom for all proceeding types except those types deemed as having a low risk of security incident as determined by the security committee. Regardless of such determination by the security committee, a second CSO should also be assigned in any proceeding when specifically requested by a judge based on a determination of risk by the judge. NOTE: This CSO should not be the same CSO assigned as responsible for an in-custody defendant(s) involved in the proceeding.

27. A judge should periodically convene a meeting with court staff to debrief on incidents that have occurred in the courtroom and to review procedures related to courtroom security. There should be an immediate debriefing following any significant security incident.
28. Provide remote video and audio linkages (and supporting infrastructure) to allow for reliable connectivity between the court and the detention center(s) as discussed Topic B-2 above.

BEST PRACTICE

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

29. For high-risk or high-visibility proceedings,[7] a minimum of two CSOs should be assigned to be present in the courtroom if no in-custody defendants are involved. If in-custody defendants are involved, a minimum of three CSO's should be assigned to be present in the courtroom.
30. For high-risk or high-visibility trials, coordinate with law enforcement and intelligence entities (e.g., Fusion Centers) to monitor social media for potential threats or protests at the court building.
31. For high-risk or high-visibility trials, coordinate with law enforcement to utilize a dog trained with the ability to detect guns, bomb materials, and other explosive contraband. Dogs may also be used to sweep courtrooms at random intervals or at the request of a judge.
32. Install two security cameras in all courtrooms:
    - One camera should be installed on the wall behind the bench facing the litigation area and public seating as described in a previous Step.
    - A second camera should be installed in the back of the public seating area facing the litigation area.
33. Install an automatic electronic lock-down mechanism on the public entrance to the courtroom in case there is a security incident in the public area outside of the courtroom.

[7] High-risk or high-visibility proceedings may be regarded as those that have the potential for personal injury, property damage, or disruption of court proceedings. Examples might include: proceedings involving more serious criminal charges, cases with multiple victims or multiple offenders; aggravated domestic violence cases; cases involving significant media coverage, demonstrations, or protests; and cases involving other significant public attention.

TOPIC B-4: CHAMBERS

PHASE ONE

1. Provide training to judges and court staff regarding personal security and safety in chambers.
2. Install a duress alarm at the judge's desk and in the chambers reception area.
3. Test duress alarms regularly (at least monthly). Train judges and court staff how and when to use the duress alarms in chambers.
4. Provide a CSO to escort judges between the chambers area and the courtroom when requested by the judge, particularly if the chambers hallway is unsecured and/or if the judge must travel through a public hallway.
5. Install blinds, preferably vertical, as interior window coverings in all chambers. Keep blinds positioned at all times so as to prevent a view into chambers from the outside.
6. Conduct daily sweeps of chambers in the morning and at the end of the day.
7. Keep entrance doors to chambers areas locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Provide advance notice to judges so they do not step outside their chambers while in-custody defendants are being escorted in the chambers hallway.
9. Position furniture in chambers with security in mind. For example, the judge's access to the exit door should not be blocked by a visitor's chair. Also, the judge's chair should be positioned, where feasible, to avoid a direct line of sight from the outside.

PHASE TWO

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

10. Establish a video intercom and remote-controlled magnetic door strike system to control access into chambers areas.
11. Plan for and conduct drills regarding emergency situations in chambers areas.
12. In locations where there are no dedicated transportation corridors for in-custody defendants, assign at least two CSOs or transport deputies to escort in-custody defendants through chambers and staff hallways, with one to clear the path ahead. The transport officer assigned direct contact with the in-custody defendant should not carry a firearm but should be armed with an intermediate weapon such as a Taser or chemical spray; the other officer should carry a firearm in a triple retention holster.
13. Install a sound and light (i.e., strobe) system in the hallways by chambers to alert judges and staff when in-custody defendants are about to be escorted through the hallway.

14. Cleaning crews should be prohibited from entering judges' chambers unsupervised at any time and should be supervised at all times by someone who is accountable to the court. Require that cleaning crews clean chambers during the end of the day when court staff members are present, rather than at night. If cleaning must be conducted at night, leave waste baskets outside locked chambers area doors. NOTE: See Topic B-6 for additional recommendations regarding access control policies and procedures for cleaning crews and vendors.
15. Install duress alarms in chambers conference room(s).

BEST PRACTICE

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

16. Install security cameras in chambers hallways that lead to chambers areas.
17. Establish a secure path (horizontally and vertically) for judges to go from chambers to courtrooms. As discussed above in Topic B-2, a separate secure path for escorting of in-custody defendants from holding cells to the courtroom without going through chambers hallways should also be established.
18. Install reflective glass or reflective film on the outside of chambers windows so that the public cannot see into these areas. Install security film on the inside of such windows. NOTE: Reflective glass and film does not prevent a view into interior spaces at nighttime and does not preclude the need for window coverings. Security film is not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.
19. Consider installing ballistic-resistant windows in areas deemed to be exposed to a specific significant threat or vulnerability (e.g., windows at ground level offices for judges and/or elected officials, presence-adjacent structures, and/or vulnerable geographic features associated with the location of the office). The recommended ballistic-resistant material for severe risk applications should meet UL Standard 752, Level IV (designed for high powered rifles).

TOPIC B-5: ACCESS OF THE PUBLIC INTO THE COURT BUILDING (WEAPONS SCREENING)

NOTE: The NCSC recommends as a Best Practice that <u>everyone</u> entering a court building should be properly screened for weapons at all times. This practice, known as "universal screening", includes judges, elected officials, court staff, attorneys, and police officers. This is recommended for the public in Topic B-5 beginning at Step 6. It is recommended for all others (e.g., judges, staff) in Topic B-6.

PHASE ONE

1. Establish only one main entrance through which the public can enter the court building.
2. Install appropriate signage at the main entrance to alert the public to what items cannot be brought into the court building (e.g., guns, knives, mace, scissors, etc.) and that all persons are subject to search by security personnel. Additionally, signage should be conspicuously placed:
    a. to inform the public of any health and safety requirements in force; and
    b. to inform the public that security cameras are operating and recording activity throughout the court building.
3. Keep all other exterior doors locked during all hours, including business hours (see also Topic B-9 for recommendations regarding security cameras at exterior doors).
4. Emergency exit crash bars should be installed on all exterior exit doors. All exit doors should be alarmed, with a ten second delay consistent with local codes. Establish signage that explains the "Exit Only" requirement. Alarms should sound at the command center and also in the immediate area of the door.
5. Conduct a security sweep of the court building in the morning before the building is open to the public and each evening after all areas of the building are closed to the public.
6. Dedicate at least one full-time CSO position to secure the main public entrance to the court building and to operate the temporary screening station.
7. Until a permanent screening station can be installed, set up a temporary table and other physical structures (e.g., stanchion ropes, dividers, etc.) to serve as the screening station.
8. Ensure that sight lines from the screening station and the building entrance/exit are unobstructed to allow for appropriate visual assessment and security response.
9. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items. The screener(s) should be provided with:
    - Training on the use of hand wand and physical search techniques.
    - The ability to contact the command center by way of a radio.
    - A weapons identification chart.
    - A list of contraband items.
    - A protocol for how to respond when weapons or contraband are discovered.
    - A listing of daily court activities.
    - Special instructions pertaining to any high-risk of high-visibility proceedings.
    - A list of phone numbers for judges, bailiffs, and other court staff.
10. Train CSO(s) in all Phase One tasks.
11. Establish a direct line of communication between law enforcement and the courts so screening personnel are aware of potentially dangerous individuals who may seek to enter the court building.

PHASE TWO

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

12. Install a magnetometer at the main door (public entrance) to the court building.
13. Per equipment manufacturer specifications, conduct a daily testing and inspection of the magnetometer. (The individual conducting the test should remove all metal from his or her person while conducting the test.) Recalibrate the magnetometer as necessary. Testing and recalibration should be conducted by an individual who has received the required training. A log should be kept of daily testing and of any necessary recalibration.
14. Train CSO(s) in all tasks added in Phase Two and provide additional security training for judges, staff, jurors, and others.
15. Install a security camera at the main door (public entrance) to the court building.
16. Assign a second CSO or contract security officer to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
17. Add a duress alarm, telephone, and gun lockers at the screening station.
18. Establish a policy that only law enforcement officers with responsibility for court security or those inside the building in an official capacity may bring a weapon into the building. Officers entering the court building on personal business (including uniformed and plain clothes officers) should not be allowed to bring in a weapon and should be required to check their weapons in a lock box at a secure location adjacent to the screening station(s). Officers that are in plain clothes on official business must wear visible identification while in the court building if they are carrying a concealed weapon.
19. Securely store contraband that has been seized at the screening station.

PHASE THREE

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

20. Install an x-ray imaging system at the public entrance screening station.
21. The second CSO or contract security officer referenced in Step 16 should be assigned as a full-time, permanent CSO or contract security officer to operate the public screening station. During slow periods, this second CSO or contract security officer can still be available for additional duties as described in Step 16 above.
22. Train CSOs and contract security officers in all tasks and provide security orientation training for judges and staff.

23. Provide screening staff with ballistic-resistant vests and require staff to wear vests at all times. (See Appendix A, item #2 for possible other CSO equipment requirements, including ballistic vests for other assignments.)
24. Install ballistic-resistant barriers at the screening station to protect screening staff.
25. Establish additional policies and procedures for Phase Three operations as follows:
    - Conduct an annual inspection and certification of x-ray imaging system. This equipment must be registered with state health and safety agencies.
    - Provide a detailed, step-by-step manual, training, and continuing education on contemporary screening procedures.

BEST PRACTICE

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

26. Assign a CSO as the third security officer to staff the public screening station: one to direct and assist visitors as they enter the screening station, one to operate the x-ray imaging system, and one to operate the magnetometer. During low traffic times, the third CSO can assume another assignment. Ideally, all CSOs should be armed, but at a minimum, one should be armed (armed CSOs should be outfitted with triple-retention holsters). All screening staff should be trained and outfitted with non-lethal defense equipment (e.g., ballistic vests). All screening staff should have body cameras and radio communication equipment.
27. Implement the following strategies into the design of security screening areas:
    - Provide an appropriate number of screenings stations[8] based on the volume of traffic regularly entering the court building.
    - Design the screening station to allow screening staff to observe the public as they enter the court building, throughout the main entrance, screening area, and lobby.
    - Provide adequate space in queuing areas to avoid overcrowding and congestion.
    - Provide re-dressing tables for visitors to organize their personal effects and belongings after going through screening. These should be located away from the screening station(s) to not interrupt the screening process for other visitors.
    - Establish clear and separate court building exit lane(s). These may be separated from the screening/queuing area with glass partitions to allow for security to

[8] In this context a screening "station" is defined as one x-ray machine plus one or more associated magnetometers.

observe the area. The exit lane(s) should be equipped with turnstiles for one way traffic.

28. If two or more public screening stations are in operation, assign an additional CSO as a supervisor to oversee operations.
29. Install reflective glass or film so that the public cannot see into the front entrance screening area but the screening station staff can see outside. Install security film on the inside of the main entry and exit doors to the court building. Such film is not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.

TOPIC B-6: ACCESS TO SECURE AREAS WITHIN THE COURT BUILDING

NOTE: The NCSC recommends as a Best Practice that everyone entering a court building should be properly screened for weapons at all times. This practice, known as "universal screening," includes judges, elected officials, court staff, attorneys, and police officers. This is recommended for the public in Topic B-5 beginning at Step 6. It is recommended for all others (e.g., judges, staff) in Topic B-6.

PHASE ONE

1. Establish a protocol for staff entry into the court building (i.e., controlled access).
    - Where staff are not required to use the main public entrance, designate one of the exterior doors to the building as a restricted entry for designated personnel (preferably staffed by an armed and qualified CSO). Access should be controlled with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through the public entrance.
    - Develop and enforce policies and procedures prohibiting staff from bringing in others (such as family members, and friends) through secure doors. "Tailgating" through secured doors should never be allowed. In this context, tailgating is when an individual(s) enters a court building by following a person who is authorized to properly gain entry with an access card or key.
2. Establish, as feasible within the court building, the concept of circulation zones to maintain separation between public, restricted, and secured areas and routes within the court building. As warranted, separation between circulation zones should run vertically (floor to floor) as well as horizontally (on the same floor). Circulations zones include the following:
    - **Public Zone:** The public circulation system provides access from the main entrance to all publicly accessible areas of the court building. All areas that require access by the public should be accessible within the public circulation zone including

courtrooms, public counter areas and court service functions, court administration, public restrooms, public elevators, and chambers reception areas.

- **Restricted Staff Zone:** The restricted circulation corridors, elevators and stairwells provide access for court staff, judges, escorted jurors, and security personnel to courtrooms, chambers, offices, and jury deliberation rooms. Judges and court staff should be able to move into work areas or courtrooms through private corridors and a private elevator without going through the public area.
- **Secure In-Custody Defendant Zone:** This zone includes in-custody defendant transport and holding areas throughout the building. The configuration of these areas should prohibit unauthorized access by the public and escape by in-custody defendants (See also Topic B-2).

3. All doors that are required to be locked, in accordance with the court building circulation zone concept should be kept secured at all times. Such doors should never be left propped open or unlocked.
4. Permit access into all secure areas of the court building only via key or electronic access device. Keys and electronic access devices should be issued and controlled pursuant to a comprehensive accountability system that has been approved under the purview of the court building security committee. Metal keys, particularly masters and grand masters, should be under close supervision at all times. The loss of metal keys for sensitive areas requires rekeying of affected locks without delay. A person should be designated to be responsible for these keys and keep a record of who has copies of these keys.
5. Conduct background checks prior to issuing a key or electronic access device to any person. Background checks should be conducted prior to employment or execution of a contract. All after-hours access should be restricted as much as possible.
6. Require, when employment is terminated, that electronic access devices be inactivated and keys turned in on the last day that the device or key holder is present in the court building and ensure that this has happened prior to the issuance of a final paycheck.
7. Document and monitor those activities where the public is required to be in the building after-hours. Set policies and procedures to ensure no unauthorized persons are in the building after-hours.
8. Establish policies and procedures for cleaning crews and any vendors including the following:
    - Conduct annual background checks for cleaning crews and any vendors granted after-hours access to the building.
    - Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court.
    - To the extent possible, courtrooms and judges' chambers should be cleaned by crews/vendors during the business day with no authorized access after-hours.

NOTE: See Topic B-4 for additional recommendations regarding cleaning of judges' chambers.

- When a contract is terminating, access devices should be immediately deactivated, and keys turned in on the last day that the device or key holder is present in the court building. Log and confirm device deactivation and key collection prior to the issuance of a final paycheck or contract payment.

PHASE TWO

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

9. Require judges and staff to prominently display badges with a photo and identifying information to allow a security officer to confirm if the individual in possession of a badge is in fact the properly authorized holder of the badge. Consider coding badges based on access level. Do not display titles on the badge to ensure that the public cannot easily identify judges.
10. Eliminate metal keys and migrate toward electronic access devices. Only maintenance staff and emergency responders should retain keys. Where keys are required in specific instances, issue double-cut, non-duplicate keys for use in emergencies or building maintenance purposes.
11. Prevent unauthorized access to critical rooms and areas such as electrical supply, roof, data centers, maintenance areas/shops, water utilities, and other building systems. Install cameras at access points to critical areas. Consider adding a two-factor authentication (e.g., using electronic access device and a unique code on a keypad) to allow a person to enter those critical rooms and areas.
12. Prevent unauthorized access to secure storage areas containing dangerous objects and substances (e.g., weapons, toxic substances, and flammable materials). When dangerous objects and substances are maintained in the court building, they should be stored in a secure area to which access is limited to those specifically identified to have access. There should be adequate ventilation, temperature controls, and fire suppression systems as required to ensure safe storage.
13. Where applicable, establish a video intercom and remote-operated magnetic door strike system to allow permitted visitor access into secure areas.

BEST PRACTICE

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

14. Establish and maintain complete separation between different zones of circulation throughout the building as described previously in Step 2 of this Topic.

15. Establish a universal screening policy. Universal screening means everyone entering the building is screened. (However, if there is not a separate entrance with a screening station for judges, then judges ought not to wait in a screening line at a public entrance.)
16. Install a magnetometer, x-ray imaging system, duress alarm, and security camera at the judge/staff entrance. Consider allowing jurors to use this entrance.
17. Assign at least one CSO to staff the judges/staff entrance. Assign two or more security officers (at least one of whom should be a CSO) to the judges/staff entrance as warranted by volume (e.g., peak hours during the day or during all normal business hours in larger, heavily trafficked court facilities).
18. For after hours, create a single access point into the court building that is secured by a CSO, or contract security officer, who checks identification and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
19. Install delayed egress units in all doors that lead from public areas to secure areas where public transit is required through the secure area in the event of fire or other emergency. The delay should be set at 15 to 30 seconds as required by local building code officials to allow time for security personnel to respond to the access breach. The units should sound an alarm at the command center and also in the immediate area of the door to alert those inside the secure area.

TOPIC B-7: OFFICES AND WORK AREAS WHERE STAFF INTERACT WITH THE PUBLIC

PHASE ONE

1. Install one or more duress alarms at each work area where staff interact with the public. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in work areas (e.g., drapes, blinds) drawn to restrict observation from outside.
3. Install Plexiglas™-type enclosures at counters where cash is handled. (See Topic C-5 for additional recommendations regarding cash handling.)
4. Ensure all public transaction counters are designed with adequate height and depth dimensions to discourage and limit attempts to jump or climb over.
5. Ensure that sensitive items such as court stamps or seals are not in reaching distance of the public standing at public transaction counters.
6. Require regular CSO patrols of all interior areas both during business hours and after hours.

PHASE TWO

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

7. Install polycarbonate (e.g., Plexiglas™) barriers over all public counters. If there is no weapons screening at the court building, or if screening is materially deficient, provide ballistic rated barriers at public counters. Ballistic-rated barriers should be installed below the counter as well as above the counter.
8. Install duress alarms strategically in the office areas behind counters.
9. Install duress alarms in all interview and conference rooms where staff meets with the public (e.g., mediation rooms and assessment interview rooms). Position furniture in these rooms with security in mind. For example, staff's access to the exit door should not be blocked by a visitor's chair.
10. Confirm that all telephone handsets allow caller ID and train staff on the functionality and protocols for the use of handsets in case of an emergency or security event.
11. Establish, where feasible, alternative safe routes for staff to exit office areas away from an active shooter or other threat. Ensure staff are aware of all exit routes available.
12. Establish safe room(s) in the court building where judges and staff can seek safety in case of a negative event. Retrofit the locking mechanism on the safe room door so that it can be locked and unlocked from the inside. Reinforce the door jamb to protect against the door being kicked in. Install a duress alarm in the safe room. Make sure that room has adequate ventilation, communication equipment, and supplies (e.g., food and water) to support a reasonable length of stay.
13. Establish clear protocols for staff dealing with clients that may have the potential for violence (e.g., those on probation) or who are required to take on sensitive assignments such as obtaining urine samples.
14. Provide mobile duress alarms to staff who have cause to come into contact with the public outside of their immediate office space (e.g., in common meeting rooms, restrooms shared with the public, etc.). Mobile duress alarms should have location tracking technology that will allow command center staff or other first responders to be able to immediately identify the location of the alarm.
15. Install doors with glass panes and sidelight windows in all mediation and conference rooms.

PHASE THREE

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

16. Install security cameras at the back of all public counters to capture the faces of members of the public conducting business at the counter.

17. Provide safe and secure waiting areas for use by victims and witnesses, protective order petitioners and respondents, and other court visitors who might be at risk of assault. Install security cameras and assign a CSO to monitor and patrol all waiting areas where there is potential for conflict.
18. Install Voice over Internet Protocol (VoIP) handsets that include emergency notification features to supplement duress alarms (e.g., push-button emergency alarm notification, two-way hands-free communication with security personnel, and audible public address notification capabilities).

BEST PRACTICE

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

19. Create dedicated interview areas for staff to meet with members of the public or clients who may have the potential for violence (e.g., those on probation) rather than having staff meet with such clients in their own staff office spaces. Interview areas should include with meeting rooms/interview booths which should be accessed separately from public and staff areas. Duress alarms should be provided in individual meeting rooms/booths. The interview area should be equipped with security cameras and monitored and patrolled by a CSO.
20. Where applicable, create separate secure drug testing areas for clients who are required to give urine samples. Public or staff restrooms should not be used for this function. Install a duress alarm in each drug testing room provided.
21. Install reflective glass or film on ground floor office windows and in any offices where there may be a higher level of threat to specific staff so that the public cannot see into these office areas. Install security film on the inside of such windows. Consider installation of ballistic rated glazing in areas deemed to be exposed to an especially high threat.
    NOTE: Reflective glass and film does not prevent a view into interior spaces at nighttime and does not preclude the need for window coverings. Security film is not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.
22. Consider installing ballistic-resistant windows in areas deemed to be exposed to a specific significant threat or vulnerability (e.g., windows at ground level offices for judges and/or elected officials, presence-adjacent structures, and/or vulnerable geographic features associated with the location of the office). The recommended ballistic-resistant material for sever risk applications should meet UL Standard 752, Level IV (designed for high powered rifles).

TOPIC B-8: JUDGES PARKING

PHASE ONE

1. Remove all signs in judges' parking areas that identify parking spaces either by name or title of judge. Any signs should simply say "reserved" along with a number as appropriate.
2. Judges should notify law enforcement officials or a designated CSO of their arrival in the morning and be offered an escort if they park in an unsecured parking area.
3. When departing for the day, if requested, judges should be provided an escort to unsecured parking areas by designated CSOs. Judges should also be provided an escort to secured parking areas by designated CSOs during high-threat proceedings or when there are heightened security concerns.
4. Install adequate lighting at the judges' parking lot.

PHASE TWO

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

5. Install security cameras with protective environmental housings in the judges' parking lot.
6. Install emergency call boxes in the judges' parking lot.
7. Fence-in the judges' parking lot using opaque materials such as brick or stone. If this is not feasible and instead a chain-link fence is used, install privacy slats in the chain-link.
8. Make sure that in-custody defendants are never afforded a view of judges getting in or out of their vehicles.
9. Provide sturdy vehicle access gates or overhead doors accessible by electronic devices. Install a video intercom connected to the command center.
10. Calibrate the timing of doors or gates to secure parking areas so that the doors or gates close in a timely fashion after entry of authorized vehicles to limit opportunities for tailgating.
11. Provide a regular CSO 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, and Two, plus add the following:

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

13. Consider installing a security booth checkpoint for access to secure parking in high-risk areas. Provide a CSO to staff the booth.

TOPIC B-9: 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.
2. Keep landscaping trimmed and neat to limit areas of concealment and reduce opportunities for undetected property damage and/or undetected access.
3. Make sure that there are clear, open, and non-congested lines of sight for all areas around the perimeter of the court building.
4. Make sure that there is adequate and unobstructed space for evacuation of the court building and for unfettered access by first responders.
5. Conduct daily security checks around the perimeter, particularly at times when the building is closed.
6. Relocate all trash receptacles, newspaper kiosks, and any other items that could be used to conceal weapons or hazardous materials to a safe distance away from the court building.
7. Keep doors locked after hours and allow access only via appropriately authorized key or electronic access devices.
8. Install signage to indicate any areas that are restricted to public access.

PHASE TWO

Continue steps in Phase One, plus add the following:

9. Install exterior security cameras overlooking the inside and outside of all exterior doors (see also Topic B-5). Cameras should be positioned to capture the face of all persons entering and exiting the building and recordings should be kept allowing CSO's, law enforcement, and court officials to review footage of building ingress/egress.
10. Install exterior security cameras around the perimeter (at each corner of the court building). Make sure that security cameras have a clear line of sight around the entire perimeter of the court building.
11. Install duress alarms and security cameras at the loading dock.

12. Install a security camera covering the driveway and exterior areas leading to the sally port (also provide a camera in the port per recommendation in Topic B-2).
13. Assign CSO exterior patrols randomly throughout the day.

PHASE THREE

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

14. Install bollards or heavy landscape features outside main entrance doors, large ground floor windows, shipping and delivery docks, and other vulnerable or critical areas.
15. Prohibit unauthorized motor vehicles from parking or accessing areas adjacent to or within "blast-proximity" of the court building. NOTE: the presence of unoccupied law enforcement vehicles parked around the perimeter of the court building can serve as a deterrent to unlawful activity.
16. Enclose and secure all exposed gas, electric, and other utilities from public access or tampering. Secure air ducts or other openings from physical intrusion and from the introduction of any toxic substance.

BEST PRACTICE

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

17. Require scheduled patrols of all exterior areas 24/7. NOTE: The schedule should be staggered and changed regularly.
18. Replace keys with an electronic access device system (except for back-up emergency) on exterior door entrances to the court building.
19. Install emergency call boxes in both staff and public parking areas around the court building.

CATEGORY C: ESSENTIAL

TOPIC C-1: EMERGENCY EQUIPMENT

PHASE ONE

1. Install an emergency, battery-generated lighting system in courtrooms, offices, and public areas to allow occupants to exit the building safely in the event of a power outage.
2. Ensure that proper and effective fire detection and suppression equipment, including, for example, alarms, sprinklers, hoses, and extinguishers, are properly installed and maintained, and are secured from tampering, vandalism, or sabotage.
3. Have periodic inspection and review of all emergency and life safety equipment and systems completed by appropriate local authorities.
4. Install automated external defibrillators (AEDs) located accessibly on each floor of the court building. Ensure staff are properly trained on the use of AEDs and related medical response procedures.

PHASE TWO

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

5. Install an emergency generator system that is properly secured and protected.
6. Test generator system monthly; keep a log of tests.
7. Determine the time-delay for emergency generators to "power-on" and install uninterrupted power supplies (UPS) for critical systems.
8. Provide basic medical/first aid supplies for all offices.

BEST PRACTICE

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

9. Install a public address system for the court building to notify occupants of emergency situations and provide instructions in case of events such as building evacuations, bomb threats, medical emergencies, in-custody defendant escapes, and unruly litigants or visitors. Pre-written and approved scripts for various incidents should be developed and approved in advance so messages can be quickly sent (see related recommendation in Topic B-1, Step 10).

TOPIC C-2: INTRUSION DETECTION SYSTEMS

PHASE ONE

1. All exterior doors and interior doors into secure areas should have basic intrusion alarm devices, that sound locally, and cover:
    - Building ingress/egress during business and after-hours.
    - Emergency exit doors during business and after-hours.

PHASE TWO

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

2. Install either glass-break or motion sensor intrusion devices that sound locally on all accessible windows, on the basement, first floor, and possibly the second floor. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

PHASE THREE

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

3. Integrate the intrusion alarms described above into the command center (or appropriate monitoring agency during after-hours) so that triggered devices sound an alarm that clearly identifies the area intruded at the court building. Alarms triggered during business hours should alert the court building's command center; when the court building is closed, the alarms should alert the control center of the appropriate responding law enforcement agency (e.g., the 911 dispatch center).

BEST PRACTICE

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

4. Integrate security cameras into the intrusion detection system described above so that cameras will be activated within the command center (or appropriate monitoring agency during after-hours) in the area(s) of intrusion.

TOPIC C-3: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

PHASE ONE

1. Provide emergency lighting in the court building, including backup generator powered lighting and lighted emergency egress signage.
2. Establish, as feasible, open hallways and lobbies with clear site lines and with no hiding spots.
3. Post floor diagrams in the hallways of the court building. Floor diagrams should be highly visible, legible, and should clearly indicate available emergency exit routes.
4. Establish egress/ingress standards regarding stairwells. For most court buildings, there should no re-entry for persons exiting into stairwells. Entry from the stairwell-side should be by controlled access only. For court buildings considered "high-rise" facilities, certain floors, as determined via security assessment and life safety analysis, may allow for re-entry.

PHASE TWO

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

20. Install security cameras in court building lobbies, hallways, stairwells, elevators, and at elevator landings.
21. Provide adequate waiting space for court visitors outside of the courtrooms so that opposing parties are not kept in close proximity. Provide a CSO to monitor waiting areas for high-risk proceedings.
22. If there are easily lifted furniture or chairs provided in public seating areas, make sure that the furniture is fastened to the floor or tied together securely.

BEST PRACTICE

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

23. Assign a CSO to regularly patrol these areas in accordance with an assigned schedule. Particular attention should be paid to patrolling high volume and high-risk areas.
24. Install adequate barriers over open atriums or stairwells to prevent someone from jumping or falling.

TOPIC C-4: JUROR SECURITY AND CIRCULATION

PHASE ONE

1. Provide jurors with court security information before they report for duty by placing information on the jury summons they receive. Such information could include by what of example:
    - Where to enter the court building.
    - What items (e.g., knives, nail files, scissors) may not be brought into the court building.
    - Not to discuss cases with anyone before and during jury service.
    - Who to contact regarding security and safety concerns or jury tampering.
2. Screen jurors as they enter the court building.
3. Give a basic security and building evacuation orientation and identification badge to jurors at the assembly area before going to the courtroom. Instruct jurors to not wear or display the identification badge off-site; and whom to notify if it is missing or lost.
4. Assign a CSO or bailiff to remain with the jury during the entire trial, including being stationed outside the deliberation room.

BEST PRACTICE

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

5. Assign a CSO to provide security inside and outside the jury assembly room when jurors are present.
6. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervisor the loading of jurors and another CSO should meet the jurors on the floor on which they disembark.
7. Install a duress alarm in each jury deliberation room and in the jury assembly room. A duress alarm may be need should a medical emergency or a violent altercation among jurors occur during deliberation,
8. Juror deliberation rooms should be located within a secure area of the court building.
9. Provide restrooms for juror use only, with no public access.
10. Provide secure ingress and egress for jurors to the court building and to their vehicles to avoid the threat of intimidation or attempt to influence.

TOPIC C-5: 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.
    - Keep cash and checks in a secure, locked area overnight.
    - Train staff on how to verify checks and reconcile fees.
    - Determine and implement industry standards for deposits.
    - If employees are responsible for depositing funds, vary scheduled departure times and routes and employees assigned and notify designated persons when departing for and completing the deposit.
2. Install protective barriers and duress alarms at cash counters.
3. Install security cameras at counters where cash is handled.
4. Use a securely installed office safe for money storage.

PHASE TWO

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

5. Install security cameras in offices where cash is handled and overlooking safes.
6. Install appropriate alarms and sensors (i.e., security, smoke, fire, extreme moisture, and motion) on safes.

BEST PRACTICE

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

7. Use an armored car service or the bank's personnel to pick up funds daily.
8. Require two people – one court staff and an armed CSO – when carrying cash in and/or out of the court building.

TOPIC C-6: SCREENING MAIL AND PACKAGES

PHASE ONE

1. Provide routine visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items.

2. Require staff to attend training on postal security, recognition points, and package identification techniques as provided by the United States Postal Service (USPS).
3. Develop and practice a response protocol with law enforcement when a package is identified as suspicious or dangerous.
4. Develop specific policies and procedures to confirm mail/package senders and recipients whether the mail/package has been tampered with.
5. Install a duress alarm in the mailroom.
6. Install a security camera in the mailroom.

PHASE TWO

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

7. Require all mail and packages to be processed through an x-ray imaging system.
8. Require everyone delivering mail or packages to pass through the magnetometer.
9. Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. Delivery people and packages should be screened through a magnetometer and x-ray machine respectively. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.

BEST PRACTICE

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

10. Establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:
    - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious) upon being received at the mailroom. This includes all USPS mail delivered and picked up by court staff from the local post office.
    - Deliveries of flowers, candy, food, gifts, etc., to any person located in a court building should be cleared through the mailroom first, be verified and vouched for by the recipient, screened as appropriate, and then delivered.

- Mailroom staff should sort incoming mail and packages off site by building, division, and/or department and prepare them for acceptance by designated representatives of each court office or division.
- Designated representatives of each court office or division should go to the mailroom, pick up mail for distribution to their offices, and identify questionable items. All authorized court and other staff mail handlers should attend training on handling suspicious mail. Local USPS or postal inspectors may conduct advanced training for state and local government agencies.

CONCLUSION

Operating a court building today is, by its very nature, a risky business. Day in and day out, court buildings are visited by a large volume of disgruntled and even law-breaking citizens. Moreover, court buildings can be seen as an important symbolic target for those in our midst who wish to wreak mischief or terror.

Court building security is not a one-time achievement. It is a serious and continuous goal requiring constant vigilance. Security is a total team effort. Every court employee is an integral part of the "security team". From court clerks to county employees to law enforcement officers, every person has a role. "See something, say something" must be the constant mantra. Judges need to be actively involved and supportive of the security effort. When judges are committed to security, a trickle-down effect on court employees will follow. When judges are not supportive of security, staff never will play their full necessary role in security efforts. The leadership role of judges cannot be overstated. Further, security must be a number one priority every single day for all those interested and involved in the process. The risks involved in court building operations are great and varied, and generally can never be eliminated. However, by exercising due diligence and devoting the appropriate attention, incidents can be both minimized and mitigated. Adhering to the stated principles and recommendations contained in this *Steps to Best Practices for Court Building Security* document will greatly assist the courts in this regard.

APPENDIX A: POLICIES AND PROCEDURES TOPICS

1. Court-specific duties and responsibilities of CSO's (and other law enforcement officers, as may be applicable[9]), to include the following by way of example:
   a) Courtrooms
      i) Ensuring a sweep is conducted of the courtroom in the morning before a proceeding is held and at the end of the day.
      ii) Maintaining courtroom order and decorum.
      iii) Constantly surveying all individuals in the courtroom.
      iv) Making sure that courtroom doors are kept properly closed and locked.
      v) Taking appropriate action in disruptive situations.
      vi) Securing or remove items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses).
   b) Chambers
      i) Conducting daily sweeps of chambers in the morning and at the end of the day.
      ii) Ensuring that chambers doors are kept properly closed and locked.
   c) Security monitoring/command center
      i) Staffing security monitoring/command center areas at all times that the building is open to the public.
      ii) After hours security monitoring.
   d) Security escorts
      i) Being available on request to provide escorts for judges. In addition, escorts should be available for staff or jurors where there is an acute security risk or vulnerability present. Examples include (but are not limited to) interior escorts when a judge leaves a chambers area for a courtroom and the pathway is unsecured, exterior escorts for judges, staff or jurors, or escorts for staff when making bank deposits.
   e) Interior and exterior patrols
      i) Ensuring daily sweeps are conducted of the court building interior and perimeter in the morning and at the end of the day.
      ii) Making sure that doors and windows are properly locked and that there are no unauthorized individuals loitering about.

[9] Where those providing security for the court building are officers of an independent law enforcement agency, such as the county sheriff, the policies and procedures listed herein pertaining particularly to such officers (e.g., duties and responsibilities, equipment, job qualifications, etc.) must be the primary responsibility of that law enforcement agency, who should consult closely with the court on all policies and procedures pertaining to court building security.

iii) Being on the lookout throughout the day for suspicious items or potentially disruptive persons.

2. Court Security Officers (and other law enforcement officers, as may be applicable) court-specific equipment, to address requirements with respect to the following equipment (along with possible additional equipment):
   a) Firearms and Ammunition.
   b) Firearm retention holsters (triple retention is recommended).
   c) Intermediate weapons (e.g., spray, Taser)
   d) Ballistic vests.
   e) Two-way radios (with earpiece).

3. Court Security Officers (and other law enforcement officers, as may be applicable) minimum job qualifications, job descriptions, performance evaluations, and other HR requirements.

4. The supervision and transport of in-custody defendants, to cover the following elements:
   a) Duty assignments for officers supervising and transporting in-custody defendants.
   b) Appropriate arming of supervising/transport officers (e.g., firearms, intermediate weapons).
   c) Required restraints ("shackling") of defendants.
   d) Procedures for transporting defendants through corridors/areas where judges, court staff or members of the public may be present.

5. Entryway Screening Policy to cover the following elements (in addition to other possible elements):
   a) Who is subject to screening? For example:
      i) The public only.
      ii) The public, including attorneys.
      iii) The public, including attorneys, and court staff.
      iv) Everyone entering the court building.
   b) Items such as weapons that are prohibited in the court building.
   c) Items that may be prohibited from the court building or courtroom, for example:
      i) Cell phones, bags, purses, containers, outerwear coats.
   d) Designation of entrances. For example:
      i) Public.
      ii) Judges.
      iii) Staff.

6. Entryway Screening Procedures to cover the following elements by way of example:
   a) Duty assignments for security officers operating the screening station.
   b) Specific screening techniques, for example:
      i) Before entering the magnetometer, must everyone do one or more of the following?
         (1) Empty pockets.
         (2) Remove belts.
         (3) Remove shoes.
      ii) Secondary screening via hand-wanding.
      iii) What items can bypass the x-ray machine.
      iv) Policies and procedures for the seizure and storage of contraband.
   c) Operation/maintenance of equipment. For example:
      i) Testing and calibration of magnetometers.
      ii) Regular inspection and certification of x-ray machines.
      iii) Demeanor of screening staff in greeting and dealing with public.

7. Who is permitted to bring a firearm into the court building, to cover the following considerations by way of example:
   a) State statutes/local ordinances regarding the right to carry a firearm.
   b) Law enforcement officers on official duty.
   c) Law enforcement officers appearing off-duty for a court proceeding in their personal capacity.
   d) Temporary storage of firearms that cannot be brought into the court building.
   e) Firearms as evidence in a proceeding.

8. Access controls that consider the following elements by way of example:
   a) Circulation zones (separate, restricted, and secured areas and routes) for the following:
   b) Judges and court staff areas (e.g., chambers, administration, jury deliberation rooms, conference rooms, staff-side of public counters, private elevators, secure stairways).
   c) In-custody defendant transport areas (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms).
   d) Public areas.
   e) Require all doors to be locked at all times in accordance with the circulation zone concept. Access control doors should never be left propped open and unsecured
   f) Keeping all exterior doors (other than the main public entrance) closed and locked at all times.
   g) After-hours access control to cover the following elements:
      i) Permitting access only via key or electronic card access.
      ii) Providing measures to govern cleaning crews and vendors who are in the court building after hours.
      iii) Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court.

   iv) To the extent possible, courtrooms and chambers should be cleaned by crews/vendors during the business day with no authorized access after-hours. Cleaning crews should never be allowed to work in judges' chambers areas unsupervised.
h) Creating a single access point into the court building that is secured where feasible by a security officer, who checks IDs and signs in all people entering the building after regular hours. As time permits, the security officer should also periodically patrol the interior and exterior of the court building.
i) Establishing where feasible full security screening operations requiring all persons to go through entryway screening.

9. Criminal background checks, to cover the following elements by way of example:
   a) Requiring criminal background checks prior to issuing a key or access card to any person.
   b) Criminal background checks should be conducted prior to employment (in the case of staff) or execution of a contract (in the case of a vendor).
   c) Criminal background checks for cleaning crews and any vendors granted after-hours access to the court building should be conducted at least annually.

10. Control over metal keys and electronic access cards/fobs, to cover the following elements by way of example:
   a) Establishing a key or access card system to control access based on a system of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience.
   b) This system should:
      i) Be under the control of a central authority.
      ii) Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination).
      iii) Require an up-to-date inventory on all access cards and keys.
      iv) Including sufficient information on the face of the access card to allow a security officer to challenge the person in possession of the card in order to make sure that the person is in fact the properly authorized holder of the card. In this regard, it is helpful for face of the access card to contain a photograph of the authorized holder.

11. Employee identification badges that include the following elements by way of example:
   a) Photo requirements.
   b) Identifying information.
   c) Requirements for displaying on person.
   d) Procedures for reporting/replacing lost or stolen badges.
   e) Integration with electronic access cards.

12. High-risk/high-visibility trials, to include the following elements (in addition to other possible elements):

a) Extensive advance planning between security officers, judges, court administration and staff, and judicial partners/stakeholders with a responsibility or interest in ensuring the safety of the proceeding.
b) Intensified intelligence gathering and sharing regarding threats.
c) Additional security measures to ensure proper separation of parties in the courtroom such as leaving the front row of the gallery vacant and/or separating family and friends of the plaintiff or prosecution from family and friends of the defendant.
d) Intensified sweeps, to include the possibility of utilizing a dog trained to detect guns, bomb materials, and other explosive contraband.
e) Additional CSOs to be present in the courtroom.
f) Pre-set procedures to anticipate and respond to disruptive behavior.

13. Duress alarms, to cover the following by way of example:
    a) Training judges and court staff on the location and functionality of duress alarms and on the protocols for use.
    b) Testing duress alarms regularly on an established schedule (at least monthly).
    c) Repairing or replacing non-functioning or malfunctioning alarms as soon as possible.

14. Security camera retention and records requirements, to cover the following elements by way of example:
    a) Whether recordings should be continuous or activated by motion or sound.
    b) How long to retain recordings.
    c) Where/how to securely store recordings.
    d) Policy regarding confidentiality of recordings.
    e) Procedures for responding to requests for recordings by law enforcement, the public, press, etc.

15. Jurors, to cover the following elements by way of example:
    a) Providing safety and security information to jurors.
    b) Entrancing and exiting for jurors.
    c) Supervision of jurors at various stages of a trial.
    d) Juror identification badges.

16. Cash handling to cover the following elements by way of example:
    a) Determining how to safeguard money during daytime work hours and overnight.
    b) Training staff on how to verify checks and reconcile fees.
    c) Determining and implementing secure practices for deposits, to include methods for transmitting deposits to a bank (e.g., armored courier service, CSO/law enforcement escort, etc.).

17. Screening mail and packages, to cover the following elements by way of example:

a) Visual inspection of all mail/packages coming into the court building, to include addressee verification and examination of suspicious items and to determine whether the mail/package has been tampered with.
b) Training staff on postal security, recognition points, and package identification techniques as provided by the United States Postal Service.
c) Response protocols with law enforcement when a package is identified as suspicious or dangerous.
d) In buildings where x-ray equipment is in place, requiring all mail and packages to be processed through an x-ray imaging system and requiring everyone delivering mail and packages to pass through a magnetometer.

18. Cell phones, to cover the following elements by way of example:
    a) Whether cell phones are permitted or prohibited in the court building or in courtrooms.
    b) Whether other portable electronic recording devices are permitted or prohibited in the court building or in courtrooms.
    c) If cell phones or other portable devices are permitted, whether photography, audio or video recording is permitted in courtrooms or elsewhere in the court building.

19. Availability of personal information online, particularly about judges.
    a) Implementing procedures for limiting or eliminating such information.

20. An Emergency Operations Plan to describe the policies and procedures dictating the response to short-term emergencies. Emergency events to be addressed should include (but not be limited) to the following:
    a) Active shooter.
    b) Suspicious and unattended packages and articles (including mail)
    c) Bomb threats and terror.
    d) Hostage situations and negotiations.
    e) Fire emergencies.
    f) Medical emergencies (AED, CPR, choking, etc.).
    g) Weather emergencies.
    h) Mechanical/ electrical emergencies.
    i) An irate or disruptive person on the premises.

21. The Emergency Operations Plan should include the following elements as appropriate:
    a) Identification of roles and responsibilities in responding to emergency events, to include identification of an incident commander during an emergency event.
    b) Lockdown, evacuation and other procedures for courtrooms, judges' chambers, in-custody holding areas, staff offices, and for all other areas of the court building.
    c) Methods for notifying judges and staff of emergencies.
    d) Lockdown and evacuation procedures for judges' chambers and courtrooms, and for all other areas of the court building.

e) Designating a floor warden on each floor to ensure proper response to emergency instructions.
f) Designating a safe area for staff to assemble and remain in place during an emergency or negative event.
g) Designating a safe area for a command center during an emergency or negative event.
h) Developing methods for notifying judges and employees of emergencies or negative events.

22. A Continuity of Operations (COOP) Plan to establish policies and procedures that ensure essential court functions are sustained during a disaster or extended emergency situation.[10]

[10] For extensive information on Continuity of Operations (COOP) Planning, see the NCSC Courts Continuity of Operations (COOP) Planning Guide and Template, which offers a step-by-step process with clear instructions for how courts may complete the key components of their COOP plan. See also the NCSC Courts Continuity of Operations Assessment Tool (C-CAT). The C-CAT was developed to help courts identify gaps in their continuity programming and identify strategies for improvement.

APPENDIX B: SECURITY STAFFING – SUMMARY OF RECOMMENDATIONS

NOTE: Staffing recommendations summarized here have been previously described in the steps, phases, topics, and categories listed previously. Refer to the individual topics for additional descriptive and phasing information.

COURT SECURITY OFFICER (CSO) STAFFING LEVELS

A CSO, as referenced in this document, is defined as an individual trained and qualified in court building security and has been specifically trained and qualified to use a firearm and intermediate weapons such as Taser, chemical spray, or restraints (e.g., handcuffs, leg restraints). An armed CSO should be outfitted with a triple-retention holster. All CSOs should be outfitted with a radio that can communicate with the command center and a body camera. The CSO assigned to the command center is not necessarily required to carry a firearm.

NOTE: It is estimated that each CSO post requires an appropriate relief factor. Typical relief factors range from 1.2 to 1.3 full-time employees to cover for sick and annual vacation, training, etc.

1. Assign CSOs to meet recommended initial staffing guidelines in the following topics:
    - At the command center (Topic B-1).
    - To escort in-custody defendants through all non-secure areas and to clear the path ahead of civilians (Topic B-2).
    - In the courtroom while there is an in-custody defendant in the courtroom (Topic B-3).
    - At the main entrance of the court building during business hours (Topic B-5).
    - On every floor that has one or more courtrooms, dedicated as a rover from one courtroom to the next (Topic B-3).
2. As additional CSOs become available, assign in the following priority per recommended phases leading up to best practice level in each relevant topic:
    - To meet recommended staffing guidelines at the command center (Topic B-1).
    - To meet recommended guidelines for transporting in-custody defendants (Topic B-2).
    - To meet the recommended staffing guidelines at the in-custody transportation control room (Topic B-2).
    - To meet recommended staffing guidelines for the courtroom (Topic B-3).
    - To meet recommended staffing guidelines at the screening station (Topic B-5).
    - To meet recommended staffing guidelines at the judges/staff entrance (Topic B-6).

- To meet recommended staffing guidelines in waiting areas for victims and witnesses, protective order petitioners and respondents, and other potential high-risk areas (Topic B-7)
- To assign random patrols for the interior and exterior of the building (Topics B-9, and C-3).

3. To achieve full recommended staffing guidelines, assign CSOs at the best practice level for the following topics:
    - Command center (Topic B-1).
    - Transporting in-custody defendants (Topic B-2).
    - Courtrooms (Topic B-3).
    - Screening stations (Topic B-5).
    - Dedicated interview areas where staff meet with members of the public (e.g., centralized probation interview area) (Topic B-7).
    - Secure parking area security booth checkpoint (Topic B-8).
    - Regular patrols of building interior and exterior (Topics B-7 and B-9).

APPENDIX C: DURESS ALARM PLACEMEMENT – SUMMARY OF RECOMMENDATIONS

NOTE: Duress alarm recommendations summarized here have been previously described in the steps, phases, topics, and categories listed previously. Refer to the individual topics for additional descriptive and phasing information.

Duress alarms, which are recommended throughout this Best Practices document, should be designed to allow judges and staff to silently send a signal to security personnel in the event of a security incident. Training should be provided to judges and staff on the functionality of duress alarms and on the protocols for use. Alarms should be tested at least monthly. Newer duress alarms are generally battery operated and controlled over a wireless network, thus reducing the need for cabling. The duress alarms should provide an audible signal to alert staff when the battery needs to be replaced. Placement of duress alarms should be in a discreet yet easily accessible location, often just below the desk of counter work area. In open office staff areas, they may be wall-mounted in an easily accessible location. Duress alarms should be integrated with other security systems as discussed in Topic B-1 (e.g., when a duress activates, an image on the appropriate camera should activate on a monitor in the command center).

DURESS ALARM LOCATIONS

1. In the in-custody transportation sally port (Topic B-2).
2. At all circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators) (Topic B-2).
3. In the courtroom at the bench and clerk's station (Topic B-3).
4. In each chamber, reception area, and chambers conference rooms (Topic B-4).
5. At public screening stations (Topic B-5).
6. At staff screening stations (Topic B-6).
7. At public service transaction counters (Topic B-7).
8. In staff offices and work areas (Topic B-7).
9. In interview and meeting rooms where staff meet with the public (Topic B-7).
10. For staff who have cause to come into contact with the public outside of their immediate office space (mobile duress alarms) (Topic B-7).
11. In each drug testing room provided (Topic B-7).
12. In the loading dock area (Topic B-9).
13. In the jury assembly room and in each jury deliberation room (Topic C-4).
14. In the mailroom (Topic C-6).

APPENDIX D: SECURITY CAMERAS – SUMMARY OF RECOMMENDATIONS

SECURITY CAMERA FUNCTIONAL CAPACITY

Courts should ensure that security cameras have sufficient and appropriate functional capacity to meet the security requirements of the court building. Functional capacity should include at least the following areas.

- Capacity to capture images in high-resolution and in color. High-resolution, digital color cameras are much better equipped to capture faces and other specific details than low-resolution, black-and-white cameras.
- Capacity to focus on targeted areas. Two types of cameras that have traditionally been used at court buildings are (a) pan/tilt/zoom cameras, and (b) fixed cameras. More recently, high-definition digital cameras with wide angle lenses, cameras with multiple lenses, fisheye, panoramic, digital pan/tilt/zoom capability have become popular. Wide-angle cameras, when equipped with sufficient image resolution quality, provide the capability for the user to focus digitally on targeted areas without losing the overall wide-angle coverage provided by the camera, thus avoiding the limitations inherent to traditional pan/tilt/zoom cameras (i.e., pan/tilt/zoom cameras might be panning and zooming at location X while another event may be happening at location Y).
- Capacity to capture images in low-light settings. Exterior cameras should have appropriate night settings, such as infrared (IR), to allow for identification of incidents and individuals in low-lighting conditions.
- Network streaming capacity. Security camera systems should utilize secure internet protocol (IP) technology to transmit video images and to provide system access and control over networks.
- Recording capacity. The camera system should have networked video recording capacity (either local or cloud-based), enabling CSOs, law enforcement, first responders, and court personnel to view incidents at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation capacity. The operation and recording function of a camera can be set to activate by either motion, sound, or by setting off duress or intrusion alarms.

SECURITY CAMERA SYSTEM MANAGEMENT AND MAINTENANCE PROTOCOLS

Courts should have written protocols in place to manage and maintain their security camera system. The written protocol should encompass at least the following topics:

- User and administrative access. Protocols should address the following types of questions:
    - What entities have access to view and download footage from the recording servers?
    - What levels of access do CSOs, law enforcement, first responder, and court staff have within the camera system?
    - What individuals have administrative rights to access and make changes to the camera system?
    - Where can the camera system be accessed (e.g., can the system be accessed remotely or only while on premise at the courthouse)?
- Camera settings and quality. Protocols should identify the following types of settings and specifications:
    - Camera resolution - Camera resolution should be set to the maximum level that the system can support (1080p is preferred). High resolution cameras typically require a large amount of data storage and bandwidth; therefore, camera resolution settings should be balanced with the capacity of supporting storage and network infrastructure.
    - Frames per second (FPS) - FPS should be set to the maximum level that the system can support (1080p is preferred). Faster frame rates typically require a large amount of data storage and bandwidth; therefore, camera frame rate settings should be balanced with the capacity of supporting storage and network infrastructure.
    - Recording intervals - A determinations should be made as to whether cameras will record continuously, or if certain cameras will have recording activated only by motion (motion activated cameras will save on storage demands).
- Maintenance. Protocols should address the following types of questions:
    - What is the protocol when cameras need to be serviced?
    - How often are audits conducted on camera or recording quality?
    - Are appropriate server and security patches being applied to recording servers and computer workstations?
    - How is the overall system being protected from a cyber intrusion?
- Request for surveillance footage. Protocols should be developed to govern requests for surveillance footage. The protocols should identify who will approve and process such requests and define which recordings would be confidential and not subject to release.

SECURITY CAMERA LOCATIONS

NOTE: Security camera recommendations summarized here have been previously described in the steps, phases, topics, and categories listed previously. Refer to the individual topics for additional descriptive and phasing information.

Security cameras should be installed in the following locations:

1. In the sally port (Topic B-2).
2. In holding cells (Topic B-2).
3. At all circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators) (Topic B-2).
4. In each courtroom (Topic B-3).
5. In hallways that access chambers (Topic B-4).
6. At security screening stations (Topic B-5).
7. At access points to critical rooms and areas such as electrical supply, roof, data centers, maintenance areas/shops, water utilities, and other building systems (Topic B-6).
8. At judges and staff entrances (Topic B-6).
9. At public service transaction counters (Topic B-7).
10. In secure waiting areas used by victims and witnesses, protective order petitioners and respondents, and other court visitors who might be at risk of assault (Topic B-7).
11. At dedicated interview areas for staff to meet with members of the public or clients who may have the potential for violence (Topic B-7).
12. In judges' parking areas (Topic B-8).
13. At the court building perimeter (Topic B-9).
14. Overlooking the inside and outside of all exterior doors (Topic B-9).
15. In staff, juror, and general public parking lots (Topic B-9).
16. At the loading dock (Topic B-9).
17. At the driveway used for transporting in-custody defendants (Topic B-9).
18. In public hallways (Topic C-3).
19. In elevators and stairwells (Topic C-3).
20. In the mailroom (Topic C-6).