



STEPS TO BEST PRACTICES *for*
COURT BUILDING SECURITY

Nathan W. Hall
Steven V. Berson
Timothy F. Fautsko
James F. O'Neil
Kevin W. Sheehan
Hon. V. Lee Sinclair, Jr.



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

ACKNOWLEDGEMENTS

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

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

Copyright © 2016 National Center for State Courts. All rights reserved.

TABLE OF CONTENTS

INTRODUCTION	1
CATEGORY A: FUNDAMENTAL	3
TOPIC A-1: SECURITY COMMITTEE	4
TOPIC A-2: POLICIES AND PROCEDURES.....	5
TOPIC A-3: THREAT AND INCIDENT REPORTING.....	9
TOPIC A-4: SECURITY TRAINING.....	10
CATEGORY B: CRITICAL	12
TOPIC B-1: COMMAND CENTER.....	12
TOPIC B-2: IN-CUSTODY DEFENDANTS	13
TOPIC B-3: COURTROOMS	14
TOPIC B-4: CHAMBERS.....	17
TOPIC B-5: ACCESS OF PEOPLE INTO COURT BUILDING	19
TOPIC B-6: PUBLIC SERVICE AREAS, COUNTERS, AND OFFICES.....	23
TOPIC B-7: JUDGES PARKING	25
TOPIC B-8: PERIMETER ISSUES.....	26
CATEGORY C: ESSENTIAL	28
TOPIC C-1: AFTER-HOURS ACCESS TO COURT BUILDING	28
TOPIC C-2: EMERGENCY EQUIPMENT.....	29
TOPIC C-3: INTRUSION DETECTION SYSTEMS.....	29
TOPIC C-4: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES).....	31
TOPIC C-5: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS.....	32
TOPIC C-6: JUROR SECURITY AND CIRCULATION.....	33
TOPIC C-7: CASH HANDLING	34
TOPIC C-8: SCREENING MAIL AND PACKAGES	35
STAFFING, DURESS ALARM, AND SECURITY CAMERA RECOMMENDATIONS INCLUDED IN THE BEST PRACTICES	37
COURT SECURITY OFFICER (CSO) STAFFING LEVELS	37
DURESS ALARMS.....	38
SECURITY CAMERAS.....	38
CONCLUSION	40

INTRODUCTION

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

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

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

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

TERMS USED IN STEPS TO BEST PACTICES

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

CATEGORY A: FUNDAMENTAL

The four topics in this category provide an essential foundation for all the other topics in *Steps to Best Practices for Court Building Security*:

- **A-1: Security Committee.** A court building security committee, meeting regularly and empowered to exercise oversight and sustain matters related to security within the court building, is a prerequisite to enable the court and its stakeholders to properly assess and address the myriad of security challenges facing court and stakeholder leadership.
- **A-2: Policies and Procedures.** A cohesive and comprehensive set of security policies and procedures is necessary to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices for Court Building Security* to further the process of developing a meaningful and effective set of policies and procedures.
- **A-3: Threat and Incident Reporting.** Threat and incident reporting is of paramount importance to the safety of judges, court employees, and the public who visit the court building. Enacting a threat and incident reporting system enables stakeholders to review and develop responses to potential negative events and reinforces security best practices.
- **A-4: Security Training.** Every single person who works in a court building has the potential to materially enhance the safety and security of his or her work environment, to be the “eyes and ears” of a workforce constantly alert to risks and threats. Judges and court staff that have been well trained on well-publicized policies and procedures provide the best means for this eyes and ears function to be effectively discharged.

TOPIC A-1: SECURITY COMMITTEE

PHASE ONE

1. Establish a court building security committee for the court building, to be chaired by a judge (preferably presiding) and having membership of at least the primary security provider and a representative of the county or other funding source.
 2. The court building security committee should operate its meetings on an action planning process of “who does what, by when, and what resources are needed.” The committee should initially meet monthly to discuss and implement recommendations contained in this report. Then, it should meet at least quarterly to discuss and propose solutions to other security problems.
 3. The judge or court administrator should meet with court security personnel and law enforcement officials on a regular basis and after any negative event to discuss security concerns and improve security at the court building.
-

PHASE TWO

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

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

PHASE THREE

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

5. Undertake a self-assessment of the security in place within the court building. Checklists with which to conduct these assessments are available from various sources, such as the National Sheriff’s Association. Assistance in conducting assessments is also available from the NCSC.
-

BEST PRACTICE

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

6. Form task forces to provide the committee with additional research and information gathering capacity. For example, an “Incident Reporting and Contraband” task force could be chaired by a member of the security committee and be responsible to set up an incident reporting and contraband analysis system that not only collects data, but actively analyzes it, reports on actions taken, and presents recommendations for change to the committee. Additional members added to various task forces could include:
 - Court staff members working in the court building, including IT staff
 - Local and state government officials
 - Local and state subject matter experts
7. Add security-based planning responsibility under the committee for court facility design, construction, and renovation projects.
8. Periodically engage an independent professional organization to conduct an audit of security measures in place for the exterior and interior of the court building.

TOPIC A-2: POLICIES AND PROCEDURES

PHASE ONE

1. Under the auspices of the court building security committee (see Topic A-1) the leadership of the court, county (or other funding body), and law enforcement should understand the need for and commit to the development and implementation of effective and comprehensive court building security policies and procedures. It is important to note that judges are particularly at the forefront of court building security. Judicial leadership is crucial in the development and implementation of security policies and procedures.

PHASE TWO

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

2. Establish a task force under the direction of the court building security committee, and with the cooperation of the appropriate law enforcement agency(s), to draft a cohesive and comprehensive set of court building security materials, to include such items as policies and procedures, operations manuals, training manuals, contingency plans, and incident reporting and risk assessment instruments and protocols. Subject matters to be covered by this comprehensive set of materials include by way of example:
 - Screening operations and protocols, including the definition of weapons and illegal items/contraband prohibited from the court building. This should also include confiscation, seizure, and removal processes for such instances.

- Management of “negative events” such as:
 - Bomb threat
 - Suspicious package
 - Fire
 - Medical emergencies
 - Violence in the courtroom or elsewhere in the court building
 - Escapes by in-custody defendants
 - Active shooter
 - Severe weather/power outage
- Management of high-visibility trials.
- Prohibiting the use of cameras/cell phones in the courtroom and prohibiting other items that could be used as weapons.
- Defining the roles of Court Security Officers (CSOs) and those responsible for court security in the building.
- Defining who has authority to bring weapons into the court building.
- Developing an emergency management manual, to include, for example, such matters as:
 - Lockdown and evacuation procedures for judges’ chambers and courtrooms, and for all other areas of the court building.
 - Designating a floor warden on each floor to ensure proper response to emergency instructions.
 - Designating a floor warden identified and trained on each floor to respond to medical emergencies (e.g., cardio pulmonary resuscitation (CPR) and use of an automated external defibrillator (AED)), while 911 is called.
 - Designating a safe area for staff to assemble and remain in place during an emergency or negative event.
 - Designating a safe area for a command center during an emergency or negative event.
 - Developing methods for notifying judges and employees of emergencies or negative events, including the use of Communication Warning Codes (see below).
 - Developing evacuation plans that everyone in the court building has been familiarized with.
- Defining specific security policies and procedures for sequestered juries.

PHASE THREE

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

3. Establish communication with employees of all stakeholders that allows for feedback and revision of security materials as follows:
 - Assign a liaison between task forces and stakeholders.
 - Provide periodic briefings in various formats to stakeholders.
 - Solicit formal feedback from stakeholders.
 - Revise court building security materials as necessary based on stakeholder feedback.
4. Officially adopt the court building security materials. Issue appropriate court orders on key security matters. To be successful, security documents need the support of judges. Court orders give legitimacy and enforceability to security policies. Examples of key matters warranting a court order include subjecting visitors to screening and ordering staff to be screened as well.
5. Publish the court building security materials. The level of detail and the audience to whom materials are published should be determined on a need to know basis.

PHASE FOUR

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

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

BEST PRACTICE

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

8. Review and update policies and procedures on a bi-annual basis and after major incidents, events, and facility renovation projects.
9. Analyze Phases Two, Three, and Four for operational effectiveness.

COMMUNICATION WARNING CODES FOR COURT BUILDINGS

The NCSC, as well as professional emergency responders, suggest that communication during an emergency be clear, understandable, and simple. Presently, state and local courts use many different warning systems and language to advise court building occupants what to do during an emergency which can be confusing.

As a result of the shootings at Columbine High School in Colorado, color codes were originally developed by a high school administrator in Olathe, Kansas. Since that time, color codes followed by verbal commands have been widely used in schools, in colleges and universities, in hospitals, and in federal and state courts to quickly direct employees what to do when an emergency occurs. The decision whether to stay or leave a court building during an emergency can often be the difference between life and death.

Realizing that clear communication and understandable, simple instructions are vital in any building emergency, courts use color codes, verbal commands, and practice drills to augment their existing evacuation procedures. Using the same color codes followed by verbal instruction in every court building will ensure that court employees can assist other building tenants, jurors, and the public how to react properly to emergencies.

RECOMMENDED COLOR CODES

- **Code Red** – **Imminent Danger**
 - An active shooter is in the court building or there is a hostage situation.
 - Get into an emergency protective posture or in a safe haven per the predetermined emergency response plan (e.g., run, hide, fight).
- **Code Orange** – **Emergency: Evacuate Building**
 - Listen to instructions from your floor warden.
 - Report to your assigned location away from the court building.
- **Code Yellow** – **Emergency: Team Responding**
 - An emergency team is responding to or is in the court building.
 - Wait for further instructions from officials.
- **Code Blue** – **Situational Awareness**
 - Cautionary: Be aware and prepared to react to danger.
 - A dangerous situation may be developing in the court building.
- **Code Green** – **Administrative/Informational**
 - Return to normal operations.
 - All is well.

TOPIC A-3: THREAT AND INCIDENT REPORTING

DEFINITIONS¹

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

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

PHASE ONE

1. Establish a policy requiring threats and incidents to be reported to the appropriate law enforcement agency and to court administration as soon as feasible, but no later than the close of business on the day in which a threat or incident occurred. The more serious the threat or incident, the more quickly it should be reported.
2. Train CSOs, judges, and staff in the court building on how to recognize threats and incidents and how to report them orally and in writing.
3. Develop and use threat and incident reporting forms and submit forms in writing to the proper authorities, at least on a monthly basis, preferably in electronic format so the designated reporters can more easily file their reports, and necessary guidance/assistance can be provided more readily. The court building security committee should receive a copy of all threat and incident reports.
4. Coordinate threat and incident information with interested parties at the state and county level. Establish a “feedback loop” that travels in all directions.

BEST PRACTICE

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

¹ Source: Implementation Plan: Courthouse Security Pilot, US. Bureau of Justice Assistance, December 18, 2009.

5. Implement a practice for regularly evaluating incident reports and making improvements based on lessons learned from reports with law enforcement officials and the chairperson of the court building security committee (and the committee's incident reporting task force).
6. Provide general feedback to staff on incidents, particularly to those who reported them (e.g., complete the feedback loop).
7. Establish an electronic system for reporting threats and incidents, to enable quick review and deployment of resources, and to enable multiple shareholders to have near-instant opportunities to review and respond. A database should be maintained on all pertinent information, to include organizational responses and any follow-up activities. Databases should be maintained at the local and state level.

TOPIC A-4: SECURITY TRAINING

PHASE ONE

1. Acknowledge that training is the glue that binds all court building security measures together. Security training needs to be frequent, repetitive and simple. Without training, staff and CSOs will never be prepared for the unexpected. Every staff member and CSO needs security training. It is essential that training be mandatory and universal. Judges in particular need to participate. Nothing gets staff to buy in to security more than a judge actively participating in security training. The judge sets the tone.
2. New judges and court staff should receive an initial court security orientation briefing that includes such topics as shooter in place and hostage-taking, emergency procedures (e.g., for fire, weather and medical emergencies), building evacuation routes, building emergency color code system, and personal safety procedures for work and home.
3. Judges and court staff should be provided with detailed instructions on reporting threats and incidents received at home or in the court building.
4. CSOs should be trained in basic court security responsibilities. CSOs should receive initial classroom instruction on courtroom security techniques, judicial and staff protection, security screening activities, firearm operation, threat de-escalation techniques and safety and weapons certification.
5. CSOs should receive basic training in emergency response, first-aid, defensive tactics, handcuffing, courtroom security, hostage situations, active-shooters, and judicial protection.
6. Command center staff should be trained in critical incident command and crisis communications.

PHASE TWO

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

7. Establish a judge and staff security continuing education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and off-site.
8. All CSOs should receive at least 24 hours of mandatory in-service training on court security each year.
9. Invite first responders, particularly the SWAT team, to do a walk-through of the court building. Encourage the SWAT team to utilize the court building as part of their own training program.

PHASE THREE

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

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

BEST PRACTICE

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

12. Establish mandatory ongoing security and safety education programs for judges and court staff that include high-profile trials, home safety techniques, travel safety tips, suspicious packages, bomb and other threats, and emergency evacuation from the court building.
13. Train judges and court staff on self-defense options, threat de-escalation techniques, and personal safety/security considerations during hostage situations.
14. Establish and schedule advanced court security training programs for CSOs to include threat de-escalation, security assessments, judicial protection, incident response, dangerous individuals, mental health issues, and high threat proceedings.

CATEGORY B: CRITICAL

TOPIC B-1: COMMAND CENTER

PHASE ONE

1. Establish a command center² in a central, secure, strategically located area of the court building with an assigned court security officer (CSO*). In smaller facilities where limited resources are available, a command center may consist simply of a monitor at a CSO's desk or workstation. The CSO assigned to the command center is not necessarily required to carry a firearm. For smaller court buildings, the monitoring function of a command center can take place close to the front entrance screening station.
2. Alarms should be constantly monitored at the command center.
3. Provide for telephone/radio communication as a point of contact between a CSO and potentially vulnerable areas of the court building, such as courtrooms and chambers.

**Note: A CSO, as referenced throughout this document, is defined as an individual trained and qualified in court building security, and has been specifically trained and qualified to use a firearm and intermediate weapons, e.g., Taser, chemical spray, or restraints (i.e. handcuffs, leg restraints). Additional CSO information can be found under the CSO Staffing Levels topic below at p. 37.*

PHASE TWO

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

4. Construct a command center in a secure area located within the court building. If this is not feasible, make sure that there is closely-restricted access to the command center, and that there is ballistic-resistant protection over the command center's doors, windows, and other areas subject to attack.

² A security command center, as referenced in this document, refers to a physical location where all security activities for the court building are controlled and all security infrastructure is monitored. A security 'command center' has a different function than an in-custody defendant 'control room' which is used to manage the transport and housing of in-custody defendants. In some court buildings, the command center and control room are combined into a single facility as a way to gain building and staffing efficiencies.

5. Install control panels and monitoring equipment for security surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch.

BEST PRACTICE

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

6. Provide additional security personnel as required to supervise and monitor command center activities. The command center should be staffed at all times when the court building is open to the public.
7. The individuals staffing a command center should not be the physical responders to a crisis. Removing them from the command center to the “fight” would result in the loss of a critical element providing situational awareness to emergency responders and staff. The situational awareness provided by the command center allows responders to make the best tactical decisions and staff to decide whether to shelter in place or run.

TOPIC B-2: IN-CUSTODY DEFENDANTS

PHASE ONE

1. Assign at least one CSO or transport deputy to escort in-custody defendants through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO to remain with defendants in the courtroom at all times.
3. In courthouses lacking a secure in-custody defendant circulation, efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum. The public should be cleared to the side of hallways and other areas prior to the escort of in-custody defendants.
4. When escorting in-custody defendants in public hallways, bystanders should be moved to the far end of the hall; not to one side or the other. When escorting in-custody defendants in a public elevator, the elevator should be cleared of all other people.
5. In-custody defendants should be properly restrained while being escorted, using handcuffs, ankle restraints, and belly chains. (They should not be handcuffed from the front.)
6. In-custody defendants should have no contact of any type, physical or verbal, with the public, family, or friends while being escorted or while in court.

PHASE TWO

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

7. Establish a control center to manage the transport and housing of in-custody defendants. The control center should include monitoring capacity and control of all doors and elevators within the secure in-custody defendant circulation area. As stated in the previous section, in some courthouses, this function may be located and managed together with the building security command center.
8. Assign a second CSO or transport deputy to escort an in-custody defendant and clear a pathway. The transport officer closest to the in-custody defendant should be armed with an intermediate weapon, e.g., Taser or chemical spray; the other officer trailing behind should be armed.
9. Make sure all holding cells and areas within the court building are appropriately structured, secured, staffed, and searched before and after each occupation.

PHASE THREE

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

10. Install security cameras along the entire in-custody defendants' escort route.
11. Establish a secure sally port for in-custody defendants entering the building

BEST PRACTICE

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

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

TOPIC B-3: COURTROOMS

PHASE ONE

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a "rover" from one courtroom to the next (unless local or state rules require additional coverage).
2. There must be at least one CSO present throughout the entire court proceeding whenever an in-custody defendant is involved.

3. Install duress alarms in the courtroom at accessible locations:
 - On top or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk's station
4. Train judges and staff on the functionality of duress alarms and on the protocols for use.
5. Test duress alarms regularly (at least monthly).
6. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. Note: In any phase, for high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband. In addition, courtrooms should be cleared and locked during a recess or when the courtroom is otherwise not in use. If individuals are allowed to stay in the courtroom during a recess, a CSO should be assigned to remain in the area.
7. Secure or remove items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers. Secure or remove all moveable furniture (e.g. moveable or folding chairs). (Such chairs can be secured by fastening them together with plastic ties around their legs.)
8. Install and then regularly test emergency lighting/fire equipment in courtrooms.
9. Always keep front and back doors to courtrooms locked when the courtroom is not in use. It should be possible to easily lock all courtroom doors from the inside.
10. The courtroom door nearest the bench should be kept closed but unlocked while court is in session to allow easy and unfettered egress for the judge at the bench. This assumes that a CSO will be present in the courtroom to prevent any unauthorized attempts to access the chambers area while court is in session. If the presence of a CSO cannot be ensured, a crash bar should be installed along with a card reader override. If a card reader is installed, it will be important to make sure judges keep their access cards handy and in close possession while in court.
11. Use proper and acceptable restraints per state law and a judge's approval on in-custody defendants. In-custody defendants, except during a jury trial or as prohibited by law, should be restrained with handcuffs, leg restraints, and belly chains.
12. Install door scopes (i.e. peepholes) for the judge's entry into the courtroom.
13. Ensure weapons as exhibits are rendered inoperable. Ammunition should always be secured in sealed evidence bags separate from any firearms.
14. Issue orders of decorum for the courtroom.
15. For high-visibility trials, and for other proceedings as warranted, institute other security measures such as leaving the front row of the gallery vacant and/or separate family and friends of the plaintiff or prosecution from family and friends of the defendant.

16. Develop policies to keep defendants seated during pleas and sentencing hearings. A seated defendant is more easily controlled and less likely to be disruptive.
17. Keep presentation tables and podiums a safe distance away from the bench.

PHASE TWO

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

18. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in the courtroom. A second CSO or transport officer should be assigned when there is an in-custody defendant present. The transport officer maintaining custody (i.e., having direct contact) of the in-custody defendant should be armed with an intermediate weapon (e.g., Taser, stun gun, or chemical spray, etc.) in lieu of a firearm. This will minimize the likelihood of an in-custody defendant obtaining a firearm during confrontations.
19. Install **one** security camera in criminal and family courtrooms. The primary security camera should be installed in the back of the bench facing the gallery. (Refer to later phases for installation of an additional camera.)
20. Holding cells for the courtroom should be properly constructed, safe for the in-custody defendants, and escape-proof.
21. Every three months, a judge should convene a meeting with court staff to debrief on incidents that have occurred in the courtroom and to review procedures related to courtroom security. There should be an immediate debriefing following any significant security incident.
22. Install bullet-resistant materials at the bench and workstations inside courtrooms. Opaque ballistic-resistant material that meets UL Standard 752, Level III, should be installed behind the vertical surfaces on the three sides of the benches and stations that are visible to the public. Bullet-resistant fiberglass panels are a cost effective material that can be field cut or factory cut to specific dimensions and installed on the backside of existing courtroom millwork.

PHASE THREE

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

23. A second CSO should be assigned to a courtroom whenever any court proceeding is being held. Whether or not there is an in-custody defendant, one CSO should be assigned for the judge and one for the courtroom. A second CSO is not ordinarily needed for civil

cases, unless specifically requested by a judge based on a determination of a higher risk involved in a particular case.

24. Install one security camera in all remaining courtrooms. The camera should be installed in the back of the bench facing the gallery.

BEST PRACTICE

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

25. For high-visibility trials, an additional CSO should be assigned to be present in the courtroom.
26. Establish a courtroom in the jail for advisements/arraignments and other hearings. Use video arraignment originating from the jail for in-custody hearings as much as permitted by state law. Video arraignment is the preferred solution to bringing in-custody defendants back and forth for settings and brief hearings.
27. Conduct sweeps of all courtrooms, including the random use of trained dogs.
28. Provide separate working offices (not in the courtroom) for clerks and others to use after courtroom proceedings have been completed.
29. Install two security cameras in all courtrooms:
 - One camera should be installed on the wall in back of the bench to monitor activities in the courtroom as described in a previous step.
 - A second camera should be installed in the back of the courtroom to monitor activities in the courtroom up to and including the well and bench area.
30. Install an automatic electronic lock-down mechanism for the courtroom.

TOPIC B-4: CHAMBERS

PHASE ONE

1. Provide training to judges and court staff regarding personal security and safety in chambers.
2. Install a duress alarm at the judge's desk and in the chamber's reception area.
3. Test duress alarms regularly – at least monthly. Train judges and court staff in how and when to use the duress alarms in chambers.
4. Escort judges when leaving a chambers area for a courtroom if the chambers hall is unsecured.
5. Keep existing chambers window coverings adjusted at all times so that activities cannot be observed from outside the court building.
6. Conduct daily sweeps of chambers in the morning and at the end of the day.

7. Keep entrance doors to chambers area locked. Keep doors to individual chambers locked when judge is not present, especially at night.
8. Provide advance notice to judges so they do not step outside their chambers while in-custody defendants are being escorted in the hallway.
9. Position furniture in chambers with security in mind. For example, the judge's access to the exit door should not be blocked by a visitor's chair. Also, the judge's chair should be positioned if at all possible to avoid a direct line of sight from the outside.

PHASE TWO

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

10. Install blinds, preferably vertical, as interior window coverings in all chambers.
11. Keep blinds positioned at all times so as to prevent a view into chambers from the outside.
12. Establish a video intercom and remote controlled magnetic door strike system to control access into chambers areas.
13. Plan for and conduct drills regarding emergency situations in chambers areas.
14. Have CSOs escort judges when leaving secure chambers and courtroom areas.

PHASE THREE

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

15. In locations where there are no dedicated transportation corridors for in-custody defendants, assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallways, with one to clear the path ahead. The transport officer assigned direct contact with the in-custody defendant should not carry a gun, but be armed with an intermediate weapon such as a Taser or chemical spray; the other officer should carry a firearm in a triple retention holster.
16. Install a sound and light (e.g., strobe) system in the hallways by chambers to alert judges and staff when in-custody defendants are about to be escorted through the hallway.
17. Install ballistic-resistant material in all accessible windows (e.g., ground level, first floor). The recommended ballistic-resistant material should meet UL Standard 752, Level IV, unless a lower level can be justified by an assessment of the risks based on such factors as adjacent structures and geographic features associated with the location of chambers. This level may be reduced based on specific security assessments.
18. Request that cleaning crews clean chambers at the end of the day when court staff is present, rather than at night. Cleaning crews should be supervised by someone who is accountable to the court.

BEST PRACTICE

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

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

TOPIC B-5: ACCESS OF PEOPLE INTO COURT BUILDINGS

PHASE ONE

1. Establish only one main entrance through which the public can enter the court building. Post signage at the main entrance that states all persons are subject to search by security. This signage should also include a listing of those items that are not allowed to be brought into the building.
 - Keep all other exterior doors locked during all hours, including business hours.
 - Emergency exit bars should be installed on all exterior exit doors. All exit doors should be alarmed, with a ten second delay consistent with local codes. Alarms should sound at the command center. Establish signage that explains the "Exit Only" requirement. (Avoid panic bar alarms with a "local alarm" feature in favor of an alarm that sounds in the command and control center.)
 - Conduct a security "sweep" of the court building in the morning before the building is open to the public and each evening after all areas of the building are closed to the public.
2. Establish protocol for entry (i.e. controlled access) through secured doors.
 - Designate one of the doors to the building (preferably staffed by an armed and qualified CSO) to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors

should not be permitted to use this door but should enter through the public entrance.

- Policies and procedures need to be developed and enforced on prohibiting staff from bringing in others (such as co-workers, family members, and friends) through secure doors. “Tailgating” through secured doors should never be allowed. In this context, tailgating is when an individual(s) enters a court building following a person who is authorized to properly gain entry with an access card or key.
3. Dedicate a full-time CSO position to secure the main public entrance to the court building.
 4. Until a screening station design can be constructed, set up a temporary table and other physical structures (e.g. stanchion ropes, dividers, etc.) to serve as the screening station. Ensure that sight lines from the screening station and the building entrance/exit are unobstructed to allow for appropriate visual assessment and security response.
 5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
 - Provide screener with ability to contact the command center by way of a radio.
 - Provide screener with a weapons identification chart.
 - Provide screener with a list of contraband items.
 - Provide screener with a listing of daily court activities.
 - Provide screener with a list of phone numbers for judges, bailiffs, and other court staff.
 6. Train CSOs in all Phase One tasks.
 7. Provide basic court security orientation training for judges and staff.
 8. Each court building should have access to at least one magnetometer that can be made available for use in high-visibility trials or other special circumstances.

PHASE TWO

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

9. Install a magnetometer at the main door (public entrance) to the court building.
10. Per system manufacturer specifications, conduct a daily testing and inspection of the magnetometer. Recalibrate the magnetometer as necessary. This should be conducted by an individual who has received the required training.
11. Train CSO(s) in all tasks added in Phase Two, plus provide additional security training for judges, staff, jurors, and others.
12. Replace keys to the court building with access cards for judges, authorized court staff, and other building tenants’ staff. Assignment of access cards must be restricted to an “as required” basis as determined under the purview of the court building security

committee. When keys are utilized, make sure they are double-cut, non-duplicate keys. Develop an inventory list for all cards and keys. When anyone's employment is terminated, cards should be deactivated and keys turned in on the last day that the card or key holder is present in the court building.

13. Install a security camera at the main door (public entrance) to the court building.
14. Install a security camera at any separate entrance(s) for judges, court employees, or attorneys.
15. Install a security camera over each locked exterior door, along with two-way audio capability.
16. Assign a second CSO* or contract security officer to assist with screening at the main entrance during high-traffic times of the day. During the day, a second CSO occasionally should conduct internal and external walk-around patrols and assist with courtroom security and security monitoring at the judge and authorized staff entrances.
17. Establish a direct line of communication between law enforcement and the courts so screening personnel are aware of potentially dangerous individuals who may seek to enter the court building.
18. Add a duress alarm, telephone, and gun lockers at the screening station.
19. Establish a policy that only law enforcement officers with responsibility for court security, or are inside the building in an official capacity, may bring a weapon into the building. Officers entering the court building on personal business (including uniformed and plain clothes officers) may not bring in a weapon and should be required to check their weapons in a lock box at a secure location adjacent to the screening station(s). Officers that are in plain clothes on official business must wear visible identification while in the court building if they are carrying a concealed weapon.

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

PHASE THREE

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

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

23. Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. Delivery people and packages should be screened through a magnetometer and x-ray machine respectively. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.
24. Provide screening staff with ballistic-resistant vests and require staff to wear vests at all times.
25. Install ballistic-resistant shields to protect screening staff.
26. Establish additional policies and procedures for Phase Three operations as follows:
 - Conduct an annual inspection and certification of x-ray imaging system. This equipment must be registered with state health and safety agencies.
 - Provide a detailed, step-by-step manual, training, and continuing education on contemporary screening procedures.

**Note: Staffing level in Phase Three is two full-time security officers at the screening station, at least one of whom is a CSO.*

BEST PRACTICE

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

27. Assign a CSO* as the third security officer to staff the public screening station: one to operate the magnetometer, one to operate the x-ray imaging system, and one to handle problems. During low traffic times, the third CSO can assume another assignment. Ideally, all CSOs should be armed, but at a minimum, one should be armed. (Armed CSOs should be outfitted with triple-retention holsters.) All screening staff should be trained and outfitted with non-lethal defense equipment. All screening staff should have body cameras and radio communication equipment.
28. If two or more public screening stations are in operation, assign a fourth CSO as a supervisor to oversee operations.
29. Install a magnetometer, x-ray imaging system, duress alarm, and security camera at the judge/staff entrance. Consider allowing jurors to use this entrance.

30. Assign at least two security officers (at least one of whom should be a CSO) to the judges/staff entrance if staff or jurors use this entrance and at peak hours during the day. Otherwise, assign at least one CSO.
31. Establish a universal screening policy. Universal screening means everyone entering the building is screened. (However, if there is not a separate entrance with a screening station for judges, then judges ought not to wait in a screening line at a public entrance.)

**Note: Staffing level in Best Practice is three full-time security officers for each public screening station, at least two of whom should be CSOs. There should also be one additional CSO to supervise multiple stations, and two security officers (at least one of whom should be a CSO) assigned to judge/staff/juror entrance.*

Best Practice Elements of Screening Stations

- Two magnetometers for each x-ray machine
- Three full-time security officers for each public screening station, at least two of whom should be CSOs
- Adequately sized for volume of traffic
- Appropriate queuing lanes
- Clear and separate entry and exit lanes
- Ballistic-resistant vests and shields
- Security camera
- Duress alarm
- Tables/chairs located away from screening station for people to get themselves back together after screening

TOPIC B-6: PUBLIC SERVICE AREAS, COUNTERS, AND OFFICES

PHASE ONE

1. Install one or more duress alarms at each public counter. Train staff on the functionality of duress alarms and on the protocols for use.
2. Keep window coverings in offices (e.g., drapes, blinds) drawn to restrict observation from outside.
3. Install Plexiglas™-type enclosures at cash counters.
4. Keep cash and checks in a secure, locked area overnight.
5. Ensure all counters are designed with adequate height and depth dimensions to discourage and limit attempts to jump or climb over.
6. If there are chairs provided in a public seating area near the counter, make sure that the chairs are fastened to the floor or tied together.

PHASE TWO

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

7. Install polycarbonate (e.g. Plexiglas™) barriers over all public counters. If there is no screening station at the court building, or if screening is materially deficient, ballistic-rated barriers should be above the counter as well as below the counter.
8. Install duress alarms strategically in the back areas of offices.
9. Install duress alarms in all mediation and conference rooms. Position furniture in mediation and conference rooms with security in mind. For example, staff's access to the exit door should not be blocked by a visitor's chair.
10. Keep cash and checks and daily change locked in a safe overnight.
11. Establish safe room(s) in the courthouse where judges and staff can seek safety in the event of a negative event. Retrofit the locking mechanism on the door so that it can be locked and unlocked from the inside. Reinforce the door jamb to protect against the door being kicked in. Install a duress alarm in the safe room.
12. Provide mobile duress alarms to staff who must share restroom facilities with the public.

PHASE THREE

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

13. Install security cameras at the back of all public counters to capture the faces of members of the public conducting business at the counter.
14. Install appropriate alarms and sensors (i.e. security, smoke, fire, extreme moisture, and motion) on safes.
15. Provide safe and secure waiting areas for victims and witnesses, those seeking protective orders, and other members of the public who might be at risk of assault.

BEST PRACTICE

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

16. Install a security camera overlooking all safes.
17. Require scheduled patrols of all interior areas 24/7.
18. Install doors with glass panes and sidelight windows in all mediation and conference rooms.

TOPIC B-7: JUDGES PARKING

PHASE ONE

1. Remove all signs in judges' parking areas that identify parking spaces either by name or title of judge. Any signs should simply say reserved along with a number as appropriate.
2. Judges should notify law enforcement officials or a designated CSO of their arrival in the morning and be offered an escort if they park in an unsecured parking area.
3. When departing for the day, if requested, judges should be provided an escort to unsecured parking areas by designated CSOs.

PHASE TWO

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

4. Fence-in the judges' parking lot using opaque materials such as brick or stone. If this is not feasible and instead a chain-link fence is used, install privacy slats in the chain-link.
5. Make sure that in-custody defendants are never afforded a view of judges getting in or out of their vehicles.
6. Install adequate lighting at the parking lot.
7. During high-threat proceedings and heightened security concerns, judges should be escorted to their vehicles and other modes of transportation.
8. Ensure the judges' parking area is equipped with appropriate security and safety lighting. Reference B-8 for additional lighting information.
9. Calibrate the timing of doors or gates to secure parking areas so that the doors or gates do not remain open for too long of a period of time.

PHASE THREE

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

10. Install call boxes and security cameras in the parking lot.
11. Provide judges and court staff a regular CSO patrol presence in the parking areas in the morning, during the lunch hour, and at close of business.
12. Install passive and active security barriers to parking areas, accessible by way of an access card or other appropriate device.

BEST PRACTICE

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

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

TOPIC B-8: PERIMETER ISSUES

PHASE ONE

1. Install appropriate signage to alert the public to what items cannot be brought into the court building (i.e., guns, knives, scissors) and that all persons are subject to search by security.
2. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness. It should also be sufficient for perimeter security cameras to capture images.
3. Keep doors locked after hours and allow access only via appropriately authorized key or access cards.
4. Employ a sound crime prevention program through environmental design by properly maintaining landscaping, trees, and shrubs to limit areas of concealment and prevent property damage and undetected access.
5. Conduct daily security checks around the perimeter, particularly at times when the building is closed.
6. Install signage to indicate any areas that are restricted to public access.
7. Relocate all trash receptacles, newspaper kiosks, and any other items that could be used to conceal weapons or hazardous materials to a safe distance away from the court building.
8. Make sure that there are clear, open, and non-congested lines of sight for all areas around the perimeter of the court building.
9. Make sure that there is adequate and unobstructed space for evacuation of the court building and for unfettered access by first responders.

PHASE TWO

Continue steps in Phase One, plus add the following:

10. Install intrusion detection systems to cover all exterior doors and accessible windows.
11. Assign CSO exterior patrols both regularly and randomly throughout the day.
12. Use window coverings and ballistic-resistant material on windows to minimize the risk of someone assaulting building occupants from the outside.

PHASE THREE

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

13. Install security cameras around the perimeter (at each corner of the court building). Make sure that security cameras have a clear line of sight around the entire perimeter of the court building.
14. Install bollards as required outside selected main entrance doors, shipping and delivery docks, over-sized ground floor windows, and other vulnerable or critical areas.
15. Prohibit motor vehicles from parking or accessing areas adjacent to or within “blast-proximity” of the court building.
16. Enclose and secure all exposed gas, electric, and other utilities from public access or tampering. Secure air ducts or other openings from physical intrusion and from the introduction of any toxic substance.
17. Require scheduled patrols of all exterior areas 24/7.

BEST PRACTICE

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

18. Install reflective glass so that the public cannot see into the front entrance screening area, but that the screening station staff can see outside.
19. Replace keys with an electronic card access system (except for back-up emergency) on exterior door entrances to the court building.
20. Install emergency call boxes in both staff and public parking areas around the court building.

CATEGORY C: ESSENTIAL

TOPIC C-1: AFTER-HOURS ACCESS TO COURT BUILDING

PHASE ONE

1. Permit access into all areas of the court building only via key or electronic card access. Keys and cards should be issued and controlled pursuant to a comprehensive accountability system that has been approved under the purview of the court building security committee.
2. Conduct background checks prior to issuing a key or access card to any person. Background checks should be conducted prior to employment or execution of a contract. All after-hours access should be restricted as much as possible. Good security should not be set aside for convenience.
3. Conduct annual background checks for cleaning crews and any vendors granted after-hours access to the building. Cleaning crews and vendors should be supervised at all times by a person who is accountable to the court. To the extent possible, courtrooms and chambers should be cleaned by crews/vendors during the business day with no authorized access after-hours. Cleaning crews should never be allowed to work in judges chambers' alone.
4. Document and monitor those activities where the public is required to be in the building after-hours. Set policies and procedures to ensure no unauthorized persons are in the building after-hours.
5. When anyone's employment is terminating, access cards should be inactivated and keys turned in on the last day that the card or key holder is present in the court building. Make sure that this has happened prior to the issuance of a final paycheck.

PHASE TWO

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

6. Eliminate the use of keys and implement the use of an access card system. Where keys are required in specific instances, issue double-cut, non-duplicate keys for use in emergencies or building maintenance purposes.

BEST PRACTICE

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

7. Create a single access point into the court building that is secured by a CSO, or contract security officer, who checks identification and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
8. Conduct full security screening operations requiring all persons to go through entryway screening.

TOPIC C-2: EMERGENCY EQUIPMENT

PHASE ONE

1. Install an emergency, battery-generated lighting system in courtrooms, offices, and public areas.
2. Install a fire extinguisher on each floor, with egress floor plans posted.
3. Install fire alarms on each floor.
4. Install an elevator(s) that meets all applicable and updated fire codes.

PHASE TWO

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

5. Install an emergency generator system that is properly fenced-in and protected.
6. Test generator system monthly; keep a log of tests.
7. Determine the time-delay for emergency generators to “power-on” and install uninterruptible power supplies (UPS) for critical systems.
8. Install automated external defibrillators (AEDs) located accessibly on each floor of the court building.

BEST PRACTICE

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

9. Ensure the fire alarm system is equipped with both a strobe and annunciator per code.

TOPIC C-3: INTRUSION DETECTION SYSTEMS

PHASE ONE

1. All exterior doors should have basic intrusion alarm devices, covering:
 - Building ingress/egress during business and after-hours.

- Emergency exit doors during business and after-hours.

PHASE TWO

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

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

PHASE THREE

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

3. Establish a fully integrated intrusion system with the following functionalities:
 - When a court building is closed, every external door should be equipped with a device that will trigger an alarm at the command center of the appropriate responding agency and identify the intruded area.
 - During business hours, every door that is kept locked should be equipped with a device that will trigger an alarm that will identify the area intruded at the command center within the building. Every locked door with an emergency exit bar should trigger an alarm whenever anyone uses it, with a ten-second delay consistent with local codes.
 - When the building is closed, the alarm should go to the control center of the appropriate responding law enforcement agency; when the building is open, the alarm should go to the building's command center.
 - Intrusion detection alarm systems should sound locally at the site of the alarm and also at the command center (or at a 911 dispatch center if the court building command center is not staffed when the court building is closed).

BEST PRACTICE

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

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

TOPIC C-4: INTERIOR ACCESS DURING BUSINESS HOURS (CIRCULATION ZONES)

PHASE ONE

1. Establish, as feasible within the courthouse, the concept of circulation zones (separate, restricted, and secured areas and routes) for the following:
 - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, staff-side of public counters, private elevators, secure stairways).
 - In-custody defendant transport (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms).
 - Public (e.g., restrict the public to public zones).
2. All doors that are required to be locked, in accordance with the court building circulation zone concept should be kept secured at all times. Such doors should never be left propped open and unsecured.
3. Have a key or access card system to control access based on a system approved by the administrative authority of who needs to have access to which areas. Cards or keys should be issued on the basis of need, not convenience. Keys should be double-cut and not subject to duplication. This system should:
 - Be under the control of a central authority.
 - Require background checks for all card or key holders.
 - Include effective procedures for retrieving keys or canceling cards when situations change (e.g., employment termination).
 - Require an up-to-date inventory on all access cards and keys.
4. Require, when employment is terminated, that cards be inactivated and keys turned in on the last day that the card or key holder is present in the court building, and to ensure that this has happened prior to the issuance of a final paycheck.

PHASE TWO

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

5. Eliminate keys and require access cards. Maintenance staff and emergency responders should retain keys.
6. Include sufficient information on the face of the access card to allow a security officer to challenge the person in possession of the card in order to make sure that the person is in fact the properly authorized holder of the card. In this regard, it is helpful for face of the access card to contain a photograph of the authorized holder.

7. Establish door scopes (peepholes) to prevent non-authorized access through secured courtroom doors.

PHASE THREE

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

8. Establish a video intercom and remote controlled magnetic door strike system to allow access into secure areas.
9. Continue to improve definition and enforcement of circulation zones.
10. Install a security camera system in all secure areas of the court building to monitor suspicious activities and inappropriate or threatening behaviors.

BEST PRACTICE

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

11. Establish and maintain complete separation among zones (e.g., in-custody defendants are not escorted through secure or public hallways; judges do not pass through public areas when going to and from their cars, through screening, and to and from chamber areas). As warranted, security zones should run vertically (floor to floor) as well as horizontally (on the same floor).

TOPIC C-5: PUBLIC LOBBIES, HALLWAYS, STAIRWELLS, AND ELEVATORS

PHASE ONE

1. Provide emergency lighting in the court building including backup generator powered lighting and lighted emergency egress signage.
2. Establish egress/ingress standards regarding stairwells, hallways, and elevators. For most court facilities, there should no re-entry for persons exiting into stairwells. Entry from the stairwell-side should be by controlled access only. For court buildings considered “high-rise” facilities, certain floors, as determined via security assessment and life safety analysis, may allow for re-entry.
3. Establish emergency procedure and evacuation diagrams. Post floor diagrams in hallways of the court building.

PHASE TWO

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

4. Designate secure and public elevators.
 - Provide secure elevator(s) for judges.
 - Provide a secure elevator for in-custody defendant transport.
5. Conduct regular CSO interior patrols by CSOs assigned to work in the court building, focusing on crowded hallways.

BEST PRACTICE

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

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

TOPIC C-6: JUROR SECURITY AND CIRCULATION

PHASE ONE

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

BEST PRACTICE

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

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

TOPIC C-7: CASH HANDLING

PHASE ONE

1. Develop and train court staff on procedures for handling cash. The procedures should:
 - Determine who should collect the money.
 - Determine how to safeguard money during the daytime work hours and overnight.
 - Train staff on how to verify checks and reconcile fees.
 - Determine and implement industry standards for deposits.
 - If employees are responsible for depositing funds, vary scheduled departure times and routes and employees assigned; and notify designated persons when departing for and completing the deposit.
2. Install protective barriers and duress alarms at cash counters.
3. Use a securely-installed office safe for money storage.

PHASE TWO

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

4. Install security cameras at counters and in offices where cash is handled.

PHASE THREE

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

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

BEST PRACTICE

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

6. Require two people – one court staff and an armed CSO – when carrying cash in and/or out of the court building.

TOPIC C-8: SCREENING MAIL AND PACKAGES

PHASE ONE

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

PHASE TWO

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

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

BEST PRACTICE

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

7. Establish a single and separate offsite screening station or location for all mail and packages delivered to the court building. It may not be feasible for smaller courts to have an offsite location dedicated exclusively to its use. Smaller courts may work with the USPS, county, or other local officials to find shared offsite space for this purpose. Best practices for operating the mailroom for larger courts include the following:
 - All mail, packages, and parcels from USPS, FedEx, UPS, DHL, and other carriers should be thoroughly screened (x-ray and explosive trace detector, if suspicious)

upon being received at the mailroom. This includes all USPS mail delivered and picked up by court staff from the local post office.

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

STAFFING, DURESS ALARM, AND SECURITY CAMERA RECOMMENDATIONS INCLUDED IN THE BEST PRACTICES

NOTE: Staffing, duress alarm, and security camera recommendations summarized here have been previously described in the steps, phases, and categories listed previously.

COURT SECURITY OFFICER (CSO) STAFFING LEVELS

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

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

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

4. As additional CSOs become available, assign in the following priority per recommended phases leading up to best practice level in each relevant topic:
 - To meet recommended staffing guidelines at screening station (Topic B-5).
 - To meet recommended staffing guidelines for the courtroom (Topic B-3).
 - To meet recommended ratios for transporting in-custody defendants (Topic B-2).
 - To assign patrols for the interior and exterior of the building (Topics B-8 and C-5).
5. Achieve full recommended staffing guidelines for the following topics:
 - Screening stations (Topic B-5).
 - Courtrooms (Topic B-3).
 - Transporting in-custody defendants (Topic B-2).
 - Regular patrols of building interior and exterior (Topics B-8 and C-5).

DURESS ALARMS

1. Install duress alarms in the courtroom and at the bench, clerk's station, and CSO station. Training should be provided on the functionality of duress alarms and on the protocols for use (Topic B-3).
2. Alarms should be tested at least monthly. Alarm batteries should be tested semi-annually.
3. Install alarms in each chamber and reception area (Topic B-4).
4. Install alarms at screening stations (Topic B-5).
5. Install alarms at public counters, cash areas, and other offices where the public has access, including those without counters (Topic B-6).
6. Provide mobile duress alarms to staff who must share restroom facilities with the public (Topic B-6).
7. Install alarms in the interview and mediation rooms that are used by members of the public.
8. Install alarms and 911 contact ability at the childcare center, if the court building includes such a center.
9. Install an alarm in the jury assembly room and in each jury deliberation room (Topic C-6).
10. Install duress alarms in the holding cell area.
11. Install a duress alarm in the loading dock area (Topic B-8).
12. Install a duress alarm in the mailroom.
13. Integrate duress alarm and camera systems so the closest security camera is automatically activated for monitoring and recording when alarms sound.

SECURITY CAMERAS

Security cameras should have the following functional capacity:

- Capacity to focus on targeted areas. Two types of cameras that have traditionally been used at court buildings are (a) pan/tilt/zoom cameras, and (b) fixed cameras. More recently, high-definition digital cameras with wide angle lenses and digital pan/tilt/zoom capability have become popular and in some places have supplanted the use of more traditional pan/tilt/zoom cameras. Wide angle cameras, when equipped with sufficient image resolution quality, provide the capability for the user to focus digitally on targeted areas without losing the overall wide angle coverage provided by the camera, thus avoiding the limitations inherent to traditional pan/tilt/zoom cameras (i.e., pan/tilt/zoom cameras might be panning and zooming at location X while another event may be happening at location Y).

- Color. This is standard in current systems. Black-and-white images cannot tell the full story. Important features are indistinguishable. Only with a color monitor can faces and other specific objects be clearly identified.
- Network streaming capacity. Security systems can utilize various kinds of technology to transmit video images and to provide system access and control. Many systems now utilize an internet protocol (IP) to transmit data and control signals over a network using a broadband link providing access to CSOs, first responders, and court personnel. Courts are encouraged to explore and adopt the ever advancing new technologies that best suit their needs and budgets.
- Recording capacity. The camera system should have digital video recording capacity enabling a CSO to view incidences at a later time. This recording function is essential for identifying perpetrators for the purpose of apprehension as well as conviction. Recordings should be retained for at least ten working days.
- Activation capacity. The operation and recording function of a camera can be set to activate by either motion or sound, or by setting off duress or intrusion alarms.

Security cameras should be installed in the following locations:

1. Security camera notification signage should be conspicuously placed to inform the public that security cameras are operating and recording activity in the area.
2. Install a digital and color security camera system at the entry screening station and in the courtroom(s) facing the gallery.
3. Install security cameras (with tamper-resistant housings) in detention areas to monitor activities in holding cells and in-custody defendant circulation areas (Topic B-2).
4. Install security cameras with protective environmental housings on the court building perimeter. Use the camera system to detect suspicious activities and incidents, and to monitor parking and adjacent areas (Topic B-8).
5. Install security cameras to monitor activity at public counters and in offices where the public may visit (Topic B-6).
6. Install security cameras at the loading dock (Topic B-8).
7. Install security cameras in hallways (Topic C-5).
8. Install security cameras in each courtroom (Topic B-3).
9. Install security cameras in elevators and stairwells (Topic C-5).
10. Install additional security cameras at security screening stations (Topic B-5).
11. Install security cameras in hallways that access chambers (Topic B-4).
12. Install security cameras in the mailroom.
13. Install security cameras in the childcare area, if such an area exists.

14. Install security cameras to cover all pathways through which an in-custody defendant may be escorted (Topic B-2).

CONCLUSION

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

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