

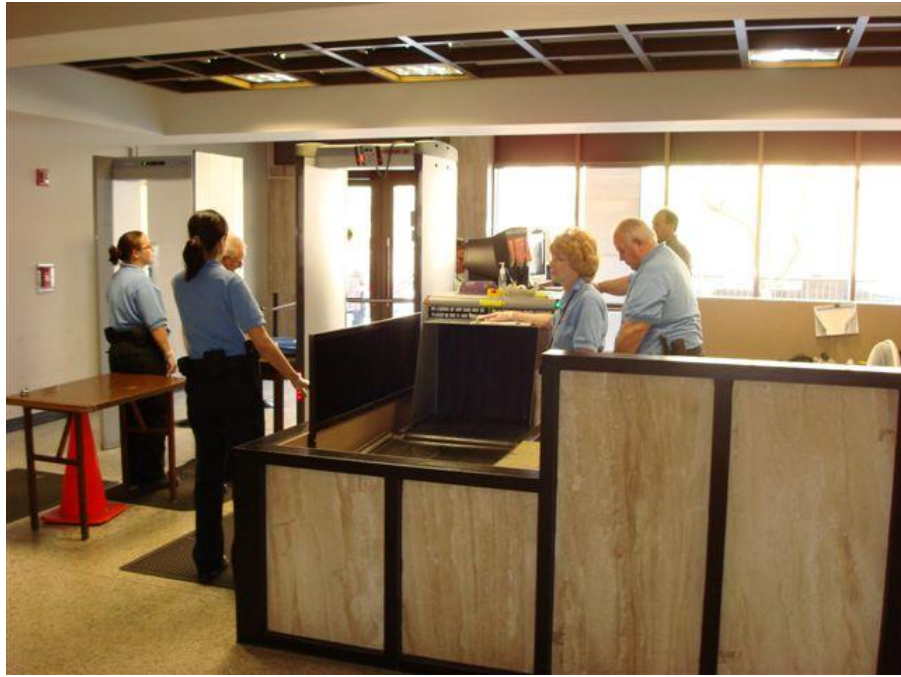


STEPS TO BEST PRACTICES FOR COURT BUILDING SECURITY

FEBRUARY 2010

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

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



Entry Screening – A Court's First Line of Defense

Acknowledgements

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

Introduction

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

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

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

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

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

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

CATEGORIES AND TOPICS

Topic

Category A: Fundamental

One	Command and control center
Two	Policies and procedures
Three	Security committee

Category B: Extremely Important

One	Access of people into court building
Two	After-hours access to court building
Three	Chambers
Four	Courtrooms
Five	Court security officer (CSO) staffing levels
Six	Duress alarms
Seven	Threat and incident reporting
Eight	In-custody defendants
Nine	Training

Category C: Very Important

One	Closed circuit television (CCTV)
Two	Emergency equipment and procedures
Three	Interior access during business hours (circulation zones)
Four	Intrusion alarms
Five	Jurors
Six	Parking (particularly for judges)
Seven	Public counters and offices

Category D: Important

One	Cash handling
Two	Exterior/interior patrols
Three	Perimeter issues
Four	Public lobbies, hallways, stairwells, and elevators
Five	Screening mail and packages

Category A: Fundamental

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

- **Command and control center.** Without such a center, the necessary and vital technological tools for court building security – closed circuit televisions (CCTV*), duress alarms, and intrusion alarms – cannot be utilized or monitored in an effective manner.
- **Policies and procedures.** Without these, there is no way to assure a thorough and consistent application of security measures aimed at making a court building reasonably safe. The development of policies and procedures is an iterative process. Reference will need to be made to the information included in *Steps to Best Practices* to inform the process of developing a comprehensive and cohesive set of policies and procedures.
- **Security committee.** Without such a committee, meeting regularly and empowered to exercise rigorous oversight on all matters relating to security within the court building, it is difficult, if not impossible, to properly assess and address the myriad of security challenges facing court leadership.

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

TOPIC A-1: COMMAND AND CONTROL CENTER

Phase One

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

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

Phase Two

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

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

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

Best Practice

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

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

TOPIC A-2: POLICIES AND PROCEDURES

Phase One

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

Phase Two

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

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

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

Phase Three

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

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

Phase Four

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

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

Best Practice

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

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

TOPIC A-3: SECURITY COMMITTEE

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

Category B: Extremely Important

TOPIC B-1: ACCESS OF PEOPLE INTO COURT BUILDING

Phase One

1. Establish only one main door through which the public can enter the court building and display a sign at the entrance clearly listing those items that cannot be brought into the court building.
 - Designate one or more of the doors to the building to be used only for one or more of the following: judges, court staff, and other building tenants, to enter with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through public entrances.
 - Keep all other exterior doors locked during business hours.
 - Emergency exit bars should be installed on all external exit doors. All exit doors should be alarmed, with ten second delay consistent with local codes. Establish signage that explains the “Exit Only” requirement.
 2. Establish protocols for entry through locked doors.
 - Tailgating* or bringing in family members/friends through these doors should not be allowed.
 - Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery. These individuals should be escorted and supervised while in the building.
- *Note: In this context, tailgating is when an individual(s) enters a court building with a person who is authorized to properly gain entry with an access card or key.*
3. Assign one CSO to guard the public entrance to the court building on a full-time basis.
 4. Set up a table or other physical structure at the public entrance to serve as a screening station.
 5. Screen people coming in the public entrance for weapons by use of a hand wand and physical search of personal items.
 - Provide screener with a weapons ID chart.
 - Provide screener with a list of contraband items.
 6. Train the CSO for all Phase One tasks described above.
 7. Provide basic court security orientation training for judges and staff.

Phase Two

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

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

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

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

Phase Three

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

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

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

Best Practice

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

22. Assign a third CSO* to operate the public screening station: one CSO to operate the magnetometer, one to operate the x-ray machine, and one to handle problems. During low traffic times, the third CSO can assume another assignment. Ideally,

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

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

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

Phase One

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

Phase Two

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

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

Best Practice

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

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

TOPIC B-3: CHAMBERS

Phase One

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

Phase Two

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

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

Phase Three

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

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

with the location of chambers. This level may be reduced based on specific security assessments.

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

Best Practice

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

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

TOPIC B-4: COURTROOMS

Phase One

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a “rover” from one courtroom to the next (unless local or state rules require additional coverage). There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.
2. Install duress alarms in the courtroom at accessible locations:
 - On top or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk’s stationTrain judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)
5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.

6. Install and then regularly test emergency lighting/fire equipment in courtrooms.
7. Always keep front and back doors to courtrooms locked when courtroom is not in use.
8. Use proper and acceptable restraints per state law on in-custody defendants.
9. Prohibit use of camera/cell phones in the courtroom and prohibit other items that could be used as weapons.

Phase Two

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

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

Phase Three

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

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

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

Best Practice

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

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

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

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

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

Phase One

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

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

Phase Two

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

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

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

Best Practice

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

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

TOPIC B-6: DURESS ALARMS

Phase One

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

Phase Two

Continue step in Phase One, plus add the following:

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

Phase Three

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

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

Best Practice

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

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

TOPIC B-7: THREAT AND INCIDENT REPORTING

Phase One

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

Best Practice

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

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

TOPIC B-8: IN-CUSTODY DEFENDANTS

Phase One

1. Assign at least one CSO or transport deputy to escort in-custody defendant(s) through all non-secure areas and to clear the path ahead of civilians.
2. Assign one CSO or transport deputy to remain with defendant(s) in the courtroom at all times.
3. Efforts should be made to modify schedules so in-custody defendants are escorted through public areas when the presence of people is at a minimum.
4. When transporting in-custody defendant(s) in public hallways, bystanders should be moved to one side of the hall. When transporting in-custody defendant(s) in a public elevator, the elevator should be cleared of all other people.

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC B-9: TRAINING

Phase One

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

Phase Two

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

4. All CSOs should receive at least 16 hours of mandatory in-service training on court security each year.

5. Establish a judge and staff security education program that deals with workplace violence and personal safety techniques, courtroom security and protection, and personal safety while at work and at home.

Phase Three

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

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

Best Practice

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

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

Category C: Very Important

TOPIC C-1: Closed Circuit Television (CCTV)

Phase One

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

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

CCTV cameras should have the following functional capacity:

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

Phase Two

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

2. Install CCTV cameras in detention areas to monitor activities in holding cells.
3. Install CCTV cameras on building perimeters and secure parking lots.
4. Install CCTV cameras to monitor activity at public counters and in offices where the public may visit.

Phase Three

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

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

Phase Four

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

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

Best Practice

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

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

TOPIC: C-2 EMERGENCY EQUIPMENT AND PROCEDURES

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

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

Phase One

1. Establish the concept of circulation zones (separate areas and routes) for the following:
 - Judges and court staff (e.g., chambers, administration, jury deliberation rooms, conference rooms, back of public counters, private elevators, secure stairways)
 - In-custody defendant transport (e.g., routes for entering and exiting the building, to and from holding areas/courtrooms)

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC C-4: INTRUSION ALARMS

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC C-5: JURORS

Phase One

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

Phase Two

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

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

Best Practice

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

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

**TOPIC C-6: PARKING
(PARTICULARLY FOR JUDGES)**

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC C-7: PUBLIC COUNTERS AND OFFICES

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

Category D: Important

TOPIC D-1: CASH HANDLING

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC D-2: EXTERIOR/INTERIOR PATROLS

Phase One

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

Phase Two

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

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

Phase Three

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

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

Best Practice

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

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

TOPIC D-3: PERIMETER ISSUES

Phase One

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

Phase Two

Continue steps in Phase One, plus add the following:

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

Phase Three

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

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

Best Practice

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

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

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

Phase One

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

Phase Two

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

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

Best Practice

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

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

TOPIC D-5: SCREENING MAIL AND PACKAGES

Phase One

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

Phase Two

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

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

Best Practice

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

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

Sample Court Building Color Codes

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

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

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

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

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

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

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