Guidelines for Implementing Best Practices in Court Building Security

Costs, Priorities, Funding Strategies, and Accountability

A Paper by the National Center for State Courts
Funded by the State Justice Institute
Grant Number SJI-09-P-125

This document was prepared under State Justice Institute (SJI) Grant SJI-09-P-125.

Table of Contents

Page

Acknowledgements

The development and publication of this report has been made possible by the continued cooperation and hard work of many people. The National Center for State Courts (NCSC) wishes to thank the State Justice Institute, who provided the funding that made this project possible. The security team of Timm Fautsko, Principal Staff at NCSC, and NCSC security consultants Steve Berson, Jim O'Neil, and Kevin Sheehan, is primarily responsible for this report and the previous development of the "Steps to Best Practices in Court Security" contained in Appendix A. Further, their work in identifying costs of these best practices has provided a useful guide for the acquisition of security staff and equipment to improve court security and public safety at local and state levels. A special thank you from the security team is extended to those members of the project's advisory committee who reviewed this publication and made important recommendations to improve the final product. Their many years of experience in the field of court security and emergency preparedness proved invaluable in *reality testing* not only the cost acquisition information, but the many steps to best practice. Without their assistance, the quality of information contained in this report would not have been possible – Frank Lalley, Judicial Security Administrator, Pennsylvania; Malcolm Franklin, Senior Manager, Emergency Response and Security, California; and Carol Price, Court Security Director, Utah. Finally, the members of the NCSC security team want to thank both NCSC editorial staff Ephanie Blair and Lorie Gomez for the many hours they spent providing quality assurance in the conformation and final editing of the report.

Introduction

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

In an effort to assist courts in the development and implementation of effective measures for court building security, the National Center for State Courts (NCSC) has developed *Steps to Best Practices*. This document, attached as the Appendix, sets forth guidelines for what constitutes best practices in various areas of court building security. It also sets forth steps in phases that can be taken toward achieving these best practices. These steps may be a useful approach for courts as they strive to prioritize and implement additional improvements in court building security. The NCSC 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. Recognizing that these measures at the best practices level can at times be costly, the *Steps* document provides 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 that can be achieved by a court over time.

To further assist courts in working with the *Steps* document, the NCSC has prepared this paper funded by the State Justice Institute. This paper includes four parts:

Part One identifies the estimated costs associated with implementing the recommendations contained in the *Steps* document.

Part Two includes a framework of priorities that a court may wish to follow in deciding when and how to implement the recommendations contained in *Steps.*

Part Three recommends strategies for seeking the funds necessary to implement the recommendations contained in *Steps.*

Part Four describes performance and accountability measures that a court may wish to utilize in order to measure the effectiveness of implementation efforts and to sustain funding for those efforts.

Court building 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. With proper attention and care, however, they can be minimized. Following the recommendations in the *Steps* document, along with the guidance provided in the four parts of this paper, can help courts minimize the risks and help keep the public, court staff, building tenants, and judicial officers more safe and secure.

Part One
Costs of Courthouse Security Improvements

The purpose of Part One is to identify the costs associated with implementing the recommendations contained in the NCSC's *Steps to Best Practices.* Almost all of the topics in the *Steps to Best Practices* document include recommendations that will require courts to spend funds on equipment or staff. These costs are set forth below by topic.

It is important to note at the outset that the costs identified here are estimates only. Costs for equipment are based on price ranges listed in catalogues, including those catalogues found through the website of American Society for Industrial Security (ASIS) International, an organization of security professionals that includes law enforcement and court security officials. The cost of equipment may vary based on brand, model, and dealer or distributor. Quantity discounts may be available through the use of county or state purchasing agreements with one or more vendors, based on the number and types of items covered by a particular order. Costs are current as of the publication of this paper.

It is important to note that in many cases the cost of installing equipment can be significant in relation to the cost of acquisition. Such installation costs are not included in the amounts indicated below and will need to be determined at the state or local level on a case-by-case basis.

The most frequently mentioned items in this analysis requiring expenditures are: (a) court security officers (CSOs) and (b) electronic systems for closed circuit television (CCTV) cameras, duress alarms, and door access systems. Costs for these items are set forth with specificity in Table A. Costs for all other referenced items are set forth by topic in Table B. When any topic listed in Table B includes expenditures for CSOs, or for CCTV, duress alarms, or door access systems, there will be a cross reference to the specific costs for these items as included in Table A.

Finally, not all courts will find their actual costs falling within the ranges indicated in the tables below. There will inevitably be outliers. A good example of this is the case of deputy sheriffs or court security officers. As noted below, the ranges indicated for these staff positions are derived from the Bureau of Labor Statistics. These ranges are calculated by the Bureau using a methodology that in effect disregards data points that fall lower than the tenth percentile or higher than the 90th percentile.

Accordingly, some larger jurisdictions, for example, may face staffing costs that exceed the higher end of the range indicated.

Table A

Item	Estimated Cost
Topic A-1: Court Security Officers (CSOs)	
County Sheriff Deputies	$30,100 - $79,700
Annual salary based on 2008 data from the Bureau of Labor Statistics. This represents a range around the national median ($54,100) from 10% at the low end to 90% at the high end.	
State Court Security Officers	$18,700 - $61,500
Annual salary based on 2008 data from the Bureau of Labor Statistics. This represents a range around the national median ($37,800) from 10% at the low end to 90% at the high end.	
Topic A-2: CCTV Camera Systems These systems include color, digital, and recording capacity.	
Tilt/Pan/Zoom – exterior camera, including housing and mounting units	$1,500 - $1,800
Tilt/Pan/Zoom – interior camera, including housing units	$1,200 - $1,500
Fixed – exterior camera, including housing and mounting units	$400 - $600
Fixed – interior camera, including housing units	$250 - $400
Digital video recorder (DVR) – 16 channel input	$3,000 - $5,000
Digital video recorder (DVR) – 32 channel input	$5,000 - $8,000
Flat-screen monitor 17-inch	$500 - $800
Flat-screen monitor 40-inch	$2,500 - $3,000
Topic A-3: Duress Alarm Systems These systems can be either hard-wired or wireless.	
Alarm control panel (hard-wired)	$250 - $300
Alarm control panel (wireless)	$250 - $300
Panic button (hard-wired)	$50 - $75
Panic button (wireless)	$75 - $125
Remote receiver (wireless)	$550 - $650
Alarm sirens (for either hard-wired or wireless system)	$50 - 75
Alarm strobe lights (for either hard-wired or wireless system)	$25 - $35
Topic A-4: Access Card Systems	
Control panel	$900 - $1,200
Card reader, per door	$500 - $600
Software to operate system	$1,200 - $1,500
Magnetic lock, per door	$250 - $350
Emergency exit button, per door	$40 - $60
Computer and printer (if no other such equipment is available in the court building for this system)	$600 - $800

Table B

Item	Estimated Cost
Topic B-1: Access of People into Court Building	
Magnetometer: single-zone units will be on the lower end of the range; multi-zone units will be at the higher end.	$2,200 - $8,600
X-ray machine	$15,000 - -$35,000
Hand-wands	$200 - $300
Court security officers (CSOs)	See Table A
Electronic access card system	See Table A
CCTV cameras	See Table A
Lock box for weapons (four compartments)	$350 - $400
Topic B-2: After-hours Access	
Electronic access card system	See Table A
Background checks: national check of criminal history and motor vehicle history. There is no charge for in-house certified user of National Crime Information Center (NCIC) or Criminal Offender Record Information (CORI).	
Topic B-3: Chambers	
Duress alarms	See Table A
Window coverings: cellular shades (24" x 36")	$55 - $65
Window coverings: vertical blinds (24" x 36")	$110 - $130
CSOs	See Table A
CCTV	See Table A
Ballistic-resistant material for windows	May require bids
Topic B-4: Courtrooms	
CSOs	See Table A
Duress alarms	See Table A
CCTV	See Table A
Ballistic-resistant material	May require bids
Video arraignment	May require bids
Topic B-5: CSO Staffing Level	
CSOs	See Table A
Topic B-6: Duress Alarms	
Duress alarms	See Table A

Topic B-8: In-custody Defendants	
CSOs	See Table A
CCTV	See Table A
Sally port	Will require bids
Secure pathway	Will require bids
Topic C-1: Closed Circuit Television (CCTV)	
CCTV	See Table A
Topic C-2: Emergency Equipment and Procedures	
Emergency generators, battery-operated, for backup lighting in courtrooms and other specific areas	$325 - $375
Fire alarm – horn and strobe light	$45 - $55
Fire extinguisher (ten pound commercial brand)	$65 - $75
Elevators to code	Will require bids
Emergency generator for court building	Will require bids
Voice-activated fire notification system – wireless, per unit	$325 - $375
CCTV	See Table A
AED	$1,700 - $1,800
Topic C-3: Interior Access	
Electronic access card system	See Table A
Viewing ports	$150 - $300
CCTV	See Table A
Videophone	$350 - $700
Topic C-4: Intrusion Alarms	
Door contacts	$70 - $80
Passive infrared motion detector strip	$90 - $110
Glass-break sensors	$70 - $80
Control panel	$225 - $275
CCTV	See Table A
Topic C-5: Jurors	
CSOs	See Table A
Topic C-6: Parking	
CSOs	See Table A
Electronic access card system	See Table A
CCTV	See Table A
Security fencing (chain link with security slats, priced per 8’ x 8’ section)	$1,200 - $1,300

Topic C-7	
Duress alarms	See Table A
CCTV	See Table A
CSOs	See Table A
Plexiglas-type enclosures, priced per square foot for 1¼-inch thick material	$60 -$65
Alarm for safe	$75 - $85
Topic D-1: Cash Handling	
Duress alarms	See Table A
CCTV	See Table A
CSOs	See Table A
Armored courier service	May require bids
Topic D-2: Exterior/Interior Patrols	
CSOs	See Table A
Topic D-3: Perimeter Issues	
Lighting	
Wall pack mount (9” x 18”)	$200 - $220
Pole unit (16-inch)	$275 - $325
High-pressure sodium bulbs	$60 - $70
Intrusion alarm	
Door contacts	$70 - $80
Passive infrared motion detector strip	$90 - $110
Glass-break sensors	$70 - $80
Control panel	$225 - $275
Bollards	
Round carbon steel – 48-inch	$1,200 - $1,300
Concrete with welded rebar – 48-inch	$375 - $425
Security fencing (chain link with security slats, priced per 8’ X 8’ section)	$1,200 - $1,300
CCTV	See Table A
CSOs	See Table A
Electronic access card system	See Table A
Topic D-4: Lobbies, Hallways, Stairwells, and Elevators	
CCTV	See Table A
CSOs	See Table A
Emergency lighting, per unit	$325 - $375
Public address system – emergency alert intercom system	$10,000 - $15,000

Topic D-5: Screening Mail and Packages	
Magnetometer: single-zone units will be on the lower end of the range; multi-zone units will be at the higher end.	$2,200 - $8,600
X-ray machine	$15,000 - $35,000
Off-site screening station	Will require bids

Part Two
Spending Priorities

As court leaders, court administrators and judges face a great responsibility and challenge in providing a safe and secure environment for those who work in or visit court buildings. The staffing levels and equipment required to provide such an environment can be costly. More likely than not, the costs for establishing and maintaining a reasonably sufficient level of court building security will exceed the amount of funding available.

Accordingly, court leadership must consider priorities very carefully when making spending decisions with respect to court building security. They will need to ask themselves: "How do we spend limited funds on security so that we get the most 'bang for the buck?' What security measures should we put in place first, what comes next, and what measures can wait until later?"

The NCSC's *Steps to Best Practices* document provides guidance with respect to spending priorities in two ways. First, it organizes topics into the following priority categories: fundamental, extremely important, very important, and important. Second, within each topic, action steps and phases are listed and recommended in priority order. While this document recommends priorities, there is no prescription for spending priorities. Court administrators, in the end, must set forth their own formula for determining the order in which items will receive security funds.

Indeed, it may not be feasible to provide a precise prescription or formula when it comes to spending priorities for court building security. Each court building is designed differently and faces a unique set of needs and resources that must be taken into account when determining the priority of security spending. In the final analysis, rather than following a rigid formula, court leadership will need to rely on its own judgment as to what is best for its court building.

It may be possible, however, to provide general guidance on priorities. This paper presents a conceptual framework that court leadership may find helpful in determining a priority order for spending on security. This conceptual framework relies on the information contained in *Steps to Best Practices* and provides a way for courts to weave

that information into a meaningful spending plan for court building security. This conceptual framework revolves around the following four goals:

- **Goal #1 – Prepare a proper foundation for court building security.**
- **Goal #2 – Prevent dangerous items and/or dangerous people from entering the court building.**
- **Goal #3 – Have the capacity to react quickly and effectively to any security incident that occurs within or around the court building.**
- **Goal #4 – Have the capacity to prevent or minimize the risk of a security incident occurring within or on the outside of the court building.**

Goal #1 – Prepare a Proper Foundation

A spending plan for court building security can be meaningful only if it is based on a solid foundation that includes a robust needs analysis. In terms of security, court leadership must have a fundamental understanding of the following: What are the risks? What are the security measures already in place? What are the significant gaps in security protection that must be put into place?

Answers to these fundamental questions can be garnered by putting into place the recommendations described by the topics under "Category A: Fundamental" in *Steps to Best Practices*. These topics are a security committee, policies and procedures, and a command and control center.

The establishment of a security committee will provide the court the wherewithal to carefully assess its security needs and determine next steps, including the development of a spending plan. Creating policies and procedures will further refine the court's direction for security protocols and enforcement and subsequent spending needs. Once these fundamentals are in place, Goal #1 is achieved. The court is ready to move forward on spending priorities relating to the remaining goals, relying on its own needs analysis along with the guidance contained in *Steps to Best Practices*.

Goals # 2 through #4 – Addressing Security Needs

Guidance from *Steps to Best Practices* in addressing Goals #2 through #4 can take different forms. All efforts will, in reality, need to be incremental. No goal will be fully satisfied initially, nor will best practices likely be achieved at once for any of the topics in

Steps to Best Practices. The incremental approach recommended here relies on the following three guidelines:

- Address the priority sequence of the goals. Do some work on Goal #2 first, then Goal #3, then Goal #4.
- Address the priorities reflected in the *Steps to Best Practices* categories. Look to the relevant topics first in category B (extremely important), then C (very important), and then D (important).
- Follow the priority sequence of the steps within each topic. Try to achieve one or more of the phases along the way to best practices within each topic.

Following this approach, court leadership will determine, based on its needs assessment, a reasonable level of additional effort it is able to make toward achieving Goal #2. It will do the same for Goals #3 and #4 consecutively. This reasonable level of effort will consist initially of taking a certain number of steps in all of the "extremely important" *Steps to Best Practices* topics relating to each goal. Court leadership will then take steps in the "very important" topics relating to each goal, then in the "important" topics relating to each goal. Once court leadership has accomplished this, it will have achieved a certain level of court building security, even though it may not have achieved the "best practices" level in any topic.

Sequence for Addressing Goals #2 - #4

	Goal #2 **Access Control**	**Goal #3** **Capacity to React**	**Goal #4** **Capacity to Prevent**
Category B **Extremely Important Topics**	First Spending Priority	Second Spending Priority	Third Spending Priority
Category C **Very Important Topics**	Fourth Spending Priority	Fifth Spending Priority	Sixth Spending Priority
Category D **Important Topics**	Seventh Spending Priority	Eighth Spending Priority	Ninth Spending Priority

Over time, and as additional funds become available, a court can repeat the effort. Starting again with Goal #1, it can reassess its current situation. Then it can go further

toward best practices for all the extremely important topics relating to Goal #2, #3, and #4 consecutively. It can go further toward best practices in the topics for the very important and important categories as well.

To illustrate this approach, in addressing Goal #2, a court will need to decide what actions it must take to keep the court building free of all unauthorized weapons or any other items that can cause injury to people or harm to property. The risk of an attack inside the court building by someone with a gun or other weapon, and the risk of explosives being set off inside the building are real and extremely serious. Expenditures of funds on staff and equipment are required to mitigate these risks.

Steps to Best Practices includes several topics relating to Goal #2. Each of these topics contains steps that will assist the court in pursing the goal of keeping the court building free from weapons and hazardous materials. To determine funding priorities in pursuit of Goal #2, a court will focus first on those topics within Category B, "extremely important." These topics are: B-1, access of people; B-2, after-hours access; B-5, CSO staffing levels; and B-7, threat and incident reporting.

Relating Topics to Goals

The court should decide how far down the steps in each of those topics it can and should go. As an example, a court might decide that it will take all the steps required to achieve the second phase of topic B-1 and all the steps required to achieve the first phase of topic B-2. Again, there is no rigid formula. Each court needs to decide what is best, based on its own unique needs and capacity. However, it can rely on guidance on the

priorities embedded in *Steps to Best Practices*, focusing on the extremely important topics first and taking the steps within each topic in priority order.

Once the court has addressed the topics in the extremely important category relating to Goal #2, it is time to move on to Goal #3 and repeat the process. Goal #3 describes the capacity to effectively and quickly respond to incidents. *Steps to Best Practices* includes topics relating to Goal #3 in the extremely important category. These are: topic B-5, CSO staffing; topic B-6, duress alarms; and topic B-9, training. Each of these topics includes steps that will enhance the capacity of the court to respond to incidents. The court should focus on those topics in category B that will help achieve Goal #3. It should go through the steps and phases of these extremely important topics as far as it reasonably can.

Next, the court should move on to Goal #4, which encompasses preventing or minimizing the risk of serious incidents. The topics in the extremely important category relating to this goal include: B-3, chambers; B-4 courtrooms; B-7, threat and incident reporting; B-8, in-custody defendants; and B-9, training.

After all of the extremely important topics have been considered, the court can return to Goal #2 and address all of the Category C (very important) topics that relate to that goal. It can then address all the Category C topics that relate to Goal #3 and #4 consecutively. Finally, the court can address all of the Category D (important) topics that relate to Goals #2, #3, and #4 consecutively.

The approach described in this part is the one recommended by the NCSC. Courts may take differing approaches. Court leadership, however, should have some structured methodology in mind. It should set goals and have a good understanding of the priority of tasks required to achieve those goals. Based on its own assessment of the unique security challenges and opportunities it faces, court leadership may wish to reconfigure the description and priority sequence of the four goals discussed above. It may also wish to reconsider the priorities embedded in the *Steps to Best Practices.* This paper, as well as the *Steps to Best Practices,* is offered as a guide to court leadership. The priorities reflected in these documents are based on the extensive security experience of the NCSC assessment team and of its group of advisors.

The following table details the relationship to each of the four goals of the many provisions contained in the *Steps to Best Practices*.

Relationship of Topics to Goals

Goal #1: Preparing a Proper Foundation	
Category A: Fundamental	
A-1	Command and control center
A-2	Policies and procedures
A-3	Security committee
Goal #2: Preventing Dangerous Items and People from Entering the Court Building	
Category B: Extremely Important	
B-1	Access of people into the court building
B-2	After-hours access into the court building
B-5	Court security officer (CSO) staffing level
B-7	Threat and incident reporting
Category C: Very Important	
C-1	CCTV cameras
C-4	Intrusion alarms
Category D: Important	
D2	Exterior patrols
D-3	Perimeter issues
D-5	Screening mail and packages
Goal #3: Capacity to React Quickly and Effectively	
Category B: Extremely Important	
B-5	CSOs
B-6	Duress alarms
B-9	Training
Category C: Very Important	
C-1	CCTV cameras
C-2	Emergency equipment and procedures
Category D: Important	
D-2	Exterior/interior patrols

Goal #4: Preventing or Minimizing the Risk of Security Incidents	
Category B: Extremely Important	
B-3	Chambers
B-4	Courtrooms
B-7	Threat and incident reporting
B-8	In-custody defendants
B-9	Training
Category C: Very Important	
C-1	CCTV cameras
C-3	Circulation zones
C-6	Parking
C-7	Public counters and offices
Category D: Important	
D-2	Exterior/interior patrols
D-3	Perimeter issues
D-4	Public lobbies, hallways, stairwells, and elevators

Part Three
Funding Best Practices:
Strategies for Working with Stakeholders

While in the final analysis courts may have ultimate responsibility for court building security, it is a responsibility that cannot be successfully discharged by courts alone. Courts acting on their own do not have the capacity or resources to fully address their own security needs. Cooperation and coordination with a host of other organizations is imperative. These other organizations are stakeholders who have a shared interest in court building security, to include the safety of their employees and the public they serve. Stakeholders may also have the capacity to help courts obtain the resources needed to make court buildings more secure. Many parties interested in the same issues and working together can serve to accomplish two significant goals for court building security:

- Developing a unified vision of what resources are needed to provide a reasonable level of security within and around a court building.
- Developing and executing a unified strategy for obtaining the resources needed.

Establishing a Security Committee

The key to getting stakeholders on board and working together is to develop and request their participation on an active and robust court building security committee. The establishment of a security committee is a fundamental recommendation in *Steps to Best Practices* (Topic A-3). Ideally, the committee should be chaired by the administrative judge. It should include a representative of each of the following stakeholders: the primary security provider, such as the county sheriff or chief of police; the clerk of court or court administrator; the district attorney and public defender; other building tenants; first responders; the bar association; county facilities manager; and local elected officials.

Conducting the Initial Committee Meetings

To achieve real progress in making court buildings more secure, members of the security committee must first come together to candidly discuss the security challenges facing them and then agree on how to develop appropriate action plans for moving forward, including funding strategies.

Toward this end, the security committee should convene a meeting involving key internal and external stakeholders for the purpose of: (1) gaining input and discussing the status of court building security and (2) examining possible funding strategies to improve court security. The meeting should have the following objectives:

- To elevate awareness and develop a shared understanding of the nature and scope of risk and the need for improved court building security.
- To develop a basic and shared understanding of the fundamental role that each stakeholder must play in order to publicly support and improve security in an effective and timely manner.
- To design a framework to garner stakeholder input and to work together within an atmosphere of accomplishment and improvement.
- To identify and evaluate the problems that in the past have been barriers to accomplishments and improvements (e.g., funding).

To achieve these objectives, this initial committee meeting will in all likelihood need to be facilitated by an outside, independent party. The facilitator, working in advance with the various key stakeholders, can help elicit their concerns and establish protocols for productive communication in these sessions. After stakeholders' input has been received on what needs to be done cooperatively to improve security in the court building, a briefing report on the meeting needs to be crafted by the committee chairperson and used to guide the court and the committee to implement change and improve security. This briefing document should then be presented to the committee and used as a roadmap to guide all stakeholders interested in improving – or charged with the responsibility for improving – court building security.

Appointment of Task Forces to the Committee

To assist the committee in its efforts to realize positive progress, various task forces, especially one on funding strategies, should be appointed. Examples of other possible task forces include, but are not limited to, such issues as:

- Policies and procedures
- Assignment of security personnel
- Facilities and equipment (e.g., CCTV)
- Building access
- Threat assessment
- Incident reporting

- Contraband analysis
- Training for judges, court staff and officers

The work product of all of the appointed task forces should culminate in a comprehensive and cohesive assessment of what security measures are in place and what additional measures are needed. It is important to note that the *Steps to Best Practices* document, the Appendix to this paper, can serve as a useful guide for assessing what is in place and what is needed. There will no doubt be many improvements that can be achieved without additional resources. Other improvements will require the expenditure of funds from existing or future budget allocations.

It is crucial that all stakeholders on the committee participate in this rigorous needs assessment process so they can be supportive of the resulting plan to improve court building security. This support will include agreeing on what is needed and being part of strategies to secure the additional funding necessary to achieve improved levels of security for the court building.

Funding Strategy

The process for securing additional funding includes fashioning and prioritizing requests arising out of the various task force assessments and recommendations. It also includes stakeholders vigorously advocating for funds from local and state sources. Moreover, other outside sources of funds to improve court building security should be identified and objectively considered, such as accessing funds from private foundations, the Office of Homeland Security, and the Bureau of Justice Assistance. It will be helpful for a coordinator at the state level to serve as a gatekeeper for the process of identifying and pursing potential outside funding sources.

Developing a Case Statement

Any successful funding strategy will rely on a solid statement that makes a convincing case for what funds are needed and why. A comprehensive, well-structured and documented needs assessment, involving the support of a broad representation of stakeholders, can help to provide the foundation for a solid case statement. The broader the net is cast to involve stakeholders and members of the community, the more allies the court will have in seeking funding.

Further, the needs assessment must lead to a rational, multi-year plan of action as part of the case statement. The action plan should reflect priorities and costs in addressing needs. It is important for stakeholders to realize that not all improvements in court building security require budget requests. As part of the action plan, those security improvements that can be accomplished with little or no money should be identified and swiftly implemented. This initial implementation of security improvements demonstrates to potential funders that the court is serious about security and that it needs additional funds to continue its quest toward achieving best practices in court security.

Those security improvements that do require significant additional funds should be carefully prioritized as part of the multi-year action plan. Part Two of this paper provides a rational basis for prioritizing spending. Such a rational basis can serve to convince funding sources that the court has been careful and thoughtful about its requests.

Other methodologies can be utilized to justify needs. Workload-based staffing models, for example, can be used to support requests for additional security staff in the court building. By analogy, staffing models developed by the NCSC have been successful in justifying the need for additional judges, court staff, district attorneys and public defenders. As these groups have experienced, a needs assessment and development of staffing standards conducted by an outside consultant may lend additional credibility to the funding requests.

Finally, the accountability measures suggested in Part Four of this paper can be helpful in putting together an effective case statement. Funders typically want to know what will be achieved or changed as a result of spending the money requested. As noted in Part Four, it can be challenging to identify what will be accomplished by adding additional security measures or improvements. In essence, a good security program is one that minimizes, or possibly eliminates, incidents by virtue of the security protocols in place. When everything seems to be working and there are no apparent risks, this makes it hard for the court to justify a request for additional funds to improve security. On the other hand, by conducting a security audit of the building and through the use of robust incident reporting and analysis, the court can demonstrate to funders the risks that need to be avoided or mitigated through the use of improved court building security.

Developing a Strategic Funding Plan

Once a convincing case statement is assembled, the security committee needs to develop a strategic plan for securing necessary funds. This is where all stakeholders' participation must be required. To achieve this objective, members of the committee must present a united front for all interested parties. To accomplish a clear assignment of responsibilities and plan of execution well-understood by all, describing who does what and when, is essential.

First, a comprehensive effort must be made to identify all possible sources of funding from various levels of government and other entities. Along with this must come a thorough understanding of the processes entailed in seeking funding from these sources. The largest piece of the funding strategy may be to seek additional funds as part of the court's (or court building tenants') next budget cycle. Another strategy for funding may be to review funds in existing budgets that can be redirected to address crucial security needs.

Second, there should be a clear understanding of who the decision makers are in terms of making funds available for security purposes. Included in this category are legislators, county commissioners, members of the town council, state and local court administrators, as well as other government officials at various levels. The challenge is to effectively convey to these decision makers why court building security is so important, as well as what additional resources are needed in order to achieve a reasonable level of security.

Conveying this message requires careful consideration of two crucial factors: (a) what protocols are involved in talking to decision makers; and (b) who is best suited to convey the message on behalf of the court. It is important that the message be neither oversold nor undersold. It is even more important that the message gets delivered by those, in a united front, who are most likely to have the ear of decision makers.

Every governmental environment has a written or unwritten set of acceptable protocols for discussing resource needs with decisions makers. There are formal avenues such as budget submissions and hearings. There are informal avenues as well, such as topic-based lunches, tours of the court building, or "ride alongs" during court days with

the judge(s).[1] Determining and utilizing the right types and numbers of avenues is critical for success.

Decision makers and their staff are typically bombarded with more information than they can reasonably process. Courts should make sure that messages about court building security are carefully crafted so the essential elements are conveyed in a crisp and cogent manner. Consequences of not funding security requests should be stated in a convincing but not alarmist fashion, although objective examples of tragedies that have occurred at other courts can be used to some extent (e.g., Reno, St. Petersburg, and others).

The final, and perhaps the most important, consideration is the determination of who delivers the message. The most significant factors to consider in selecting messengers are (a) subject matter knowledge, (b) credibility, and (c) relationships. The messengers must first know the subject matter they are presenting. Second they must have a reputation for absolute credibility in order for the message to be well received. Finally, a determination needs to be made as to who among the stakeholders and other interested parties has the best relationship with various decisions makers. Again, decision makers and their staff can be overwhelmed by those wanting their attention. They are most likely to listen to and be receptive of messages from those with whom they have a good personal relationship and can trust.

Overlaying the two factors of protocols and messengers is the absolute need for a unified message. For a funding strategy to be successful, all stakeholders need to present a united front and remain in "lock-step" on messages. Any discord among stakeholders or discrepancy in messages will only serve to confuse decision makers and provide a reason not to fund.

In order to ensure effective execution of the funding strategy, it will be helpful to designate one person, under the auspices of the security committee, to be the primary contact person and coordinator of information and committee members for executing the funding strategy. This one person should have the responsibility to make sure that: (a) the message is well-crafted; (b) the right messengers are using appropriate protocols to

[1] In a "ride along" program, a decision maker, such as a legislator, may spend the day with a judge. This gives the legislator an opportunity to observe first hand a life in the day of a judicial officer.

talk to the right decisions makers; and (c) there is a unified front among all stakeholders at all times.

Conclusion

In an uncertain world, court leaders can be certain of two things: (a) there are inherent and serious risks associated with court building operations, and (b) the level of resources needed to provide a reasonable level of security to protect against these risks will be hard to come by. Given these realities, it is imperative for court leaders to develop and implement effective funding strategies. This is a daunting challenge. The approach outlined in this paper will prove helpful to court leaders as they face this challenge.

Part Four
Accountability and Performance Measures

Introduction

When budget shortfalls occur in state courts,[2] difficult *cutback management* decisions are made by municipal, county, and state officials across the country. Funding bodies in most states look closely at performance and accountability of programs when making difficult budget decisions. Court security programs are often targets of these decisions. Therefore, in order to at least maintain the status quo, it is incumbent on courts and the providers of court security programs to be accountable, to document performance, and to objectively prove the worth of court security as an essential function. When demonstrated in courts, accountability more likely than not means there is leadership in place that acknowledges that the measurable productivity of programs is absolutely necessary for continued funding. Continuation and expansion of successful programs in state government happens in those programs that continually measure performance in order to explain, report, and be held accountable for low or non-performance.

The underpinnings that support accountability are the performance, achievement, or accomplishment of a duty or responsibility. In essence, performance can be defined as that which is performed or accomplished, a deed or act which supports the mission of the court and can be measured. In court security programs, this performance is demonstrated not only by the implementation of security policies and procedures, but also by the performance of actions, i.e., protecting the public and employees in a courthouse.

One of the major difficulties with respect to accountability and performance measures in court security programs is that success is difficult to define and to measure. For example, if there are no incidents occurring in the courthouse or in courtrooms, some funding bodies, managers, and employees may contend that they are safe; and they may ask why a lot of money should be spent on court security. Conversely, others, although they may support having security in their court and feel comfortable with its presence,

[2] According to the Center for Budget and Policy Priorities reported updated December 18, 2009, 43 states have imposed cuts in state spending. On January 3, 2010, according the Associated Press (AP), 36 states are facing severe budget shortfalls in 2010.

often have little understanding or knowledge of how court security works or what it really does to protect them.

For example, not many judges or court employees connect the fact that a court security officer confiscated a person's knife coming into the building with the result that a threat has been reduced. Since the threat of having a knife in the courthouse has been taken away, it is impossible to know whether or not the individual possessing the knife and entering the courthouse would have used it to do harm. Courts and their security providers nationwide are challenged to prove that their security program is effective, that it is necessary for public safety, and that the program needs to continue receiving funding. Courts and their security providers need to be able to prove to their funding bodies that court security is an essential function and should not be cut back. It is analogous to why the Transportation Services Administration (TSA) cannot change its universal screening policy and let people bypass screening stations to board planes unfettered.

The increasing demand for accountability and proof of performance in lean economic times not only puts pressure on courts to develop objectives to prove accountability, but to establish performance measurement systems as well. Courts that want to maintain funding levels for their security programs, in cooperation with their security providers, are now making efforts to build capacity in both areas. Such capacity has traditionally been limited by the lack of objective instruments to evaluate the quality of the security programs and the adequacy of staffing needed to support effective security.

The Need for Data

Funding bodies must have performance measurement data in order to make the correct decisions on the allocation of resources. Objective and unbiased information as to what security measures are being accomplished, what needs additional attention, and what parts of the program are performing at targeted expectation levels, is vital to appropriate resource allocation decisions. Court security programs must compete for funding with other programs in the court, the municipality, the county, or the state. In this day and age, the competition for limited funds is fierce. The collection of data and

subsequent analysis of that data is a must. The following are tools security professionals can use to measure a program's capabilities and effectiveness and, in the long run, to demonstrate the need to continue funds for existing programs and obligate additional funds for expansion.

The Need for Policy and Procedures

In state or municipal courts, most policy statements that provide an umbrella of protection for court employees are written, approved, and promulgated locally or by the state's supreme court. These policy statements often turn into procedures for the establishment and operation of court security programs. A search of the Internet will provide access to numerous state court security handbooks, as well as policies on such wide-ranging subjects as: what is considered contraband in courthouses; cell phone use in courtrooms; who is required to submit to entryway screening; and the membership and range of responsibilities of members of a court's security committee. Such policies and procedures must be subject to performance measures. Not only should these measures be based on the court's mission, vision, goals, and objectives, but the results of the measurement should be linked to the need for resources to properly manage, and if necessary expand, the existing security program.

The Need for Oversight

Oversight of court security programs is necessary to determine accountability and to measure performance. Although oversight usually comes from the managers of court security providers, e.g., the sheriff, it is important to involve all the members on the court security committee – the stakeholders in the system. When committee members become involved in the oversight process, they can regularly monitor policies, procedures, staffing needs, incident reporting, and threat analysis. They can also review response times for such events as building evacuation, hostage-taking, or other emergencies. When all of the parts needed for oversight are in sync, then effective measurement of program performance can more easily occur.

Having oversight in place is also important for the providers of court security to establish measurements and test protocols for assessing their operations and the physical status of their security programs. Hence, the security provider, in cooperation with the

court security committee, can expect consistent application of procedures, testing of performance measures, and accountability.

The Need for Performance Measure

In order to determine and prove success, performance measures of various aspects of the court's security program need to be established. In general there are three types of performance measures: input, output, and outcome. Input measures are tangible and are the basis of the program's components. Such items as budget, staffing, hardware, and the size of the physical plant are not only measurable, but they also relate to certain program goals or objectives. For example, the courts may have as an objective a fully staffed and functional screening station consisting of three court security officers, a magnetometer, and an x-ray machine. This is a best practice guideline that can be adopted as an objective and can be measured. On the other hand, output measures are the products and services produced by the court security programs that can be observed and measured. These measures are what the funding body evaluates when deciding on budget allocation or cutbacks. These are measures that providers, in cooperation with the security committee, can use to prove program effectiveness. Examples of output measures include such items as the number of people screened per day, the amount and types of contraband confiscated, or the number of incidents recorded and successfully responded to. These output measures establish program accountability and provide funders the answers to their questions, such as: "Are we at risk?" "What are you doing to keep us safe?" "What are we getting in return for the money we spend?" "Why shouldn't we reduce your funding request?"

When it comes to protecting people and property, court security programs need to be able to measure such items as the time it takes to evacuate the building and the time it takes to respond to activated courtroom duress alarms or to incidents inside or outside the courthouse. This is achieved through the use of testing – practice evacuations and practice responses to duress alarms. The use of testing and the collection of resulting data is what can fundamentally defend security programs. Equipment must be tested to make sure duress alarms are active, that CCTV cameras work, that magnetometers are properly calibrated, that contraband is collected and incidents are being analyzed, that

courtroom and personal safety training is provided for judges and court staff, that court security officers are adept at reading x-ray machines, that intrusion alarms are monitored after hours, and that the courthouse is protected after hours from intruders. Testing should occur regularly and randomly (test weapons through magnetometers), but the testing process used must follow established protocols. Identifying, establishing, testing, and proving the effectiveness of output measures is at the heart of program success. Without them, court security programs that cannot prove their essential functions are at the mercy of the ebb and flow of good and bad funding times.

The Need for Outcome Measures

Outcome measures represent the impact the court security program has on public and employee safety. In essence, the measurement of outcomes proves the occurrence or non-occurrence of an undesired situation. For example, if a gunman is killed trying to shoot his way into a courthouse by court security officers at entryway screening (St. Petersburg, Florida, May 7, 2008) is the court security program successful? When a man enters a federal courthouse (Las Vegas, Nevada, January 4, 2010), kills a court security officer, injures a United States Marshal, does not make his way past screening and into the courthouse to harm others, and is ultimately shot and killed across the street from the courthouse, did entryway screening work? The vast majority of people will answer these questions with a resounding, "Yes, thankfully!"

Outcome measures are used to assess how well individual tasks are performed in relationship to overall program goals. These measures can support various program objectives. The regular audit or assessment of court facilities and the monitoring of subsequent improvements made is one way to reduce risk. For example, reducing public entrances to the courthouse from several to one by implementing the steps to best practice guidelines contained in the Appendix, supports the goal of improving public and employee safety. Or when measuring emergency preparedness, it is important to determine as an outcome measure how often table top exercises or practice evacuations drills are conducted. This event can be measured by how participants behave during the exercise or how evacuees react during the drill. Do they assume their role and correctly react during the exercise? Do they leave the building(s) in a timely fashion and assemble

at the correct location? Do all judges and jurors comply with the drill? Another outcome measure should involve cost. In relation to cost, the following questions should be answered: Are court security officers (CSOs) being reduced or expanded over time? Why? Are volunteer court security officers being trained and used in the program to reduce costs? Do judges and court staff receive regular safety training? Is the presence of a uniformed CSO directly related to the reduction of incidents?

The Need to Implement Performance Measures

Using performance measures to substantiate accountability is useful for all decision makers involved in the operation and success of the court security program. For example, performance measures can be used to determine whether the program is supporting the strategic direction of its funders. Performance measures may be used in many other ways by: (1) demonstrating effectiveness to program managers and court security committee members; (2) assessing emergency preparedness capabilities; (3) evaluating and maintaining equipment; and, most important, (4) determining the adequacy of resources to support operational and legal requirements necessary to measure court security program success. Physical (security) related performance measures provide valuable information that not only can be used to support funding requests or to accomplish program objectives, but also to identify areas for improvement and to increase public and employee safety. It is important to note that physical performance measures are always more tangible, and in a sense easier to measure, than process items such as program support and attitude.

The Need for Incident and Threat Reporting

In order for accountability and performance measures to be effective and credible, they must be supported by a comprehensive and robust incident and threat reporting system. All incidents and threats within a court building must be promptly reported. Those observing incidents or receiving threats must be aware of how to report and to whom to report. All reports of incidents and threats must be reviewed at an appropriate level and action taken by responsible parties as warranted. Information contained in incident and threat reports, to include actions taken in response, should be analyzed and catalogued on an ongoing basis. This information can provide a solid foundation for

performance and accountability measures by identifying in a systemic way the security challenges a court faces and the resources required to meet those challenges.

Conclusion

The proof of accountability through the use of performance measures can be instrumental as an integral component of an effective case statement for funders, as described in Part Three. Those making decisions on funding typically want to know what will be achieved or changed as a result of spending the money requested. In essence, they want to know what the problem was and how the work of the program resulted in a solution.

For court security programs in eras of budget reductions, proving accountability through use of performance measures is the most important way to demonstrate to funding bodies that the provision of security hardware and staffing is working and that as a result their investment in the security program is working. Objective determination of the success of input, output, and outcome measures not only will document the effectiveness of providing public safety to funding bodies, but it will also provide security providers and court leadership a management tool as well as a basis for documentation of future needs. Finally, using performance measures to establish accountability will ensure consistency of operations and cost-effective program management, improve the overall management and protection of court facilities, and ensure the safety of employees and the public at-large.[3]

[3] Portions of this part of the report on Accountability and Performance Measures are extracted from an article entitled *Use of Physical Security Performance Measures* by the Department of Homeland Security.

Appendix

Steps to Best Practices

STEPS TO BEST PRACTICES FOR COURT BUILDING SECURITY

JANUARY 2010

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

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

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

These 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 intrusions 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.

.

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.

**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.*

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 to include:
        - 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 on 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 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 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 station

    Train judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)
5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.

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

Phase Two

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

10. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in a 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 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 codes 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 varying 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 supervisor 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 evacuation 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.