



Judicial Council of California · Administrative Office of the Courts

455 Golden Gate Avenue · San Francisco, California 94102-3688

www.courts.ca.gov

REPORT TO THE JUDICIAL COUNCIL

For business meeting on December 14, 2012

Title

Court Security: Final Report of the Court
Emergency Response and Security Task
Force

Agenda Item Type

Action Required

Effective Date

N/A

Rules, Forms, Standards, or Statutes Affected

None

Date of Report

November 30, 2012

Recommended by

Court Emergency Response and Security
Task Force
Hon. Frederick Paul Horn, Chair

Contact

Malcolm Franklin, 415-865-8830
malcolm.franklin@jud.ca.gov
Michael I. Giden, 818-558-4802
michael.giden@jud.ca.gov

Executive Summary

The Court Emergency Response and Security Task Force has evaluated court security—including emergency planning, continuity of operations, and personal security issues—and presents its recommendations for the Judicial Council to manage, maintain, and enhance security in the courts. The task force recommends that the council receive its report, maintain the AOC Office of Security, and create a Court Security Advisory Committee to promote the security of judges, court employees, and the public they serve.

Recommendation

The Court Emergency Response and Security Task Force recommends that the Judicial Council immediately:

1. Receive the final report of the Court Emergency Response and Security Task Force (Final Report; see Attachment B).

2. Direct the Administrative Director of the Courts to maintain the AOC Office of Security within the Judicial and Court Operations Services Division and to change its name to the “AOC Office of Court Security.” (Recommendation 1 of the Final Report.)
3. Establish a Court Security Advisory Committee to oversee and consult with the AOC Office of Security and to advise the Judicial Council on issues related to court security and emergency planning. (Recommendation 2 of the Final Report.)
4. Charge the Court Security Advisory Committee with the following duties and responsibilities:
 - a. Perform all the duties and responsibilities identified in rule 10.34 of the California Rules of Court with a focus on court security and emergency response planning (Recommendation 2 of the Final Report);
 - b. Review the scope of work, organization, and appropriate staffing for the AOC Office of Security, and make a recommendation to the Judicial Council regarding any appropriate changes (Recommendations 1 & 2 of the Final Report);
 - c. Review and evaluate options for implementing a statewide threat and incident reporting program for the judicial branch, taking into account current law and practices and the necessity of coordinating with the California Highway Patrol (CHP) and sheriffs’ and marshals’ offices. The program should provide for uniform reporting, assessment, and sharing of information regarding threats and incidents across the branch statewide and in coordination with the CHP and sheriffs’ and marshals’ offices (Recommendation 3 of the Final Report);
 - d. Continue to review and evaluate the viability and usefulness of developing and establishing court security classification and staffing guidelines (Recommendation 4 of the Final Report); and
 - e. Review and evaluate the process for preparing and submitting court security plans, as required by Government Code section 69925, and make recommendations to the council to facilitate and increase trial court compliance with that statute (Recommendation 5 of the Final Report).
5. Direct the AOC Office of Security to (1) disseminate information to educate judges and judicial branch staff about the emergency planning tools, programs, and assistance that it makes available to the courts; and (2) further develop the emergency planning tools. (Recommendation 6 of the Final Report.)

Adoption of these recommendations is necessary for the Judicial Council to manage, maintain, and enhance security in the courts with accountability and transparency.

Previous Council Action

Chief Justice Ronald M. George (Ret.) established the Judicial Council’s Court Emergency Response and Security Task Force, effective August 15, 2007, appointing Judge Frederick Paul Horn as its chair. In forming the task force, the Chief Justice brought together representatives from existing statewide advisory groups that had been formed to address security and emergency planning in the trial and appellate courts. A roster of the members is attached to this report (Attachment A).

The charge of the task force is to evaluate emergency planning, continuity of operations, court security, and personal security issues and to develop recommendations for the Judicial Council to manage, maintain, and improve security in the courts through statewide systems and progressive initiatives to increase efficiency, effectiveness, and cost-saving measures in California and to provide a final report of recommendations to the Judicial Council at the end of its term. The task force was originally scheduled to complete its work and report to the council by August 2010; but that deadline was extended to allow the task force to address events that had an impact on the task force’s recommendations, including court security realignment, the Strategic Evaluation Committee’s report, and the restructuring of the AOC. The attached report is the first report the Judicial Council has received from the task force.

At its August 31, 2012, meeting, in response to the final report of the Strategic Evaluation Committee’s review of the AOC, the Judicial Council directed the Administrative Director of the Courts “to return to the Judicial Council with an analysis, defining the necessary emergency response and security functions for the branch and a recommendation on the organizational plan for council approval.”¹ That recommendation is due to the Judicial Council at its December 14, 2012, meeting.² Judge Jahr (a member of the task force until he resigned following his appointment as Administrative Director of the Courts) requested that the task force complete its report and submit it to the Judicial Council at its December 14, 2012, meeting to coincide with the submission of his recommendation regarding the AOC Office of Security. This will permit the Judicial Council to have the full benefit of the task force’s expertise and its dedicated and extensive work on court security when it assesses the future of the AOC Office of Security.

Rationale for Recommendation

Unlike virtually any other institution in our society, the judicial branch has the authority to compel citizens to attend court involuntarily, as jurors, witnesses, or parties in connection with civil, family, criminal, dependency, or other pending cases. The task force submits that with this authority comes a moral responsibility to provide a civilized environment uncorrupted by threats and avoidable risks to those who enter the courthouse. Assuring the security of the public who come to California’s courthouses, and the judges and court employees who serve that public, is

¹ Judicial Council of Cal., mins. (Aug. 31, 2012), p. 11, Attachment 3, p. 52.

² *Ibid.*

necessary to achieve the fundamental judicial branch goal of providing equal access to justice for all Californians.

The recommendations of the task force are based on the experience and expertise of judicial officers and court administrators from around the state who have been involved in the administration of court security in California. The members of the task force worked together and individually over a five-year period to assess the current status of court security in the branch and to consider what recommendations to the Judicial Council would best enhance the security and safety of the public, judicial officers, and court employees. Six recommendations represent the culmination of that work.

The specific rationale for each of those recommendations is set forth at length in the Final Report.

Comments, Alternatives Considered, and Policy Implications

Due to the necessity of addressing issues of immediate concern to the Judicial Council—i.e., the disposition of the AOC Office of Security—the task force has not circulated its Final Report for public comment. Moreover, most of the recommendations are for the proposed Court Security Advisory Committee to pursue. As the Court Security Advisory Committee proposes new programs or procedures, it is anticipated that such proposals will be circulated for public comment prior to the Judicial Council’s review.

The alternatives considered by the task force and the policy implications of the recommendations are discussed in the Final Report.

Implementation Requirements, Costs, and Operational Impacts

At present, no additional requirements, costs, or operational impacts are associated with maintaining the AOC Office of Security because the task force is not recommending any substantive changes. The cost of operating the Court Security Advisory Committee may represent a savings over the cost of operating the task force and the two working groups on court security, which will likely soon be disbanded. Implementation requirements and costs on other recommendations will need to be provided once specific proposals are developed to carry out the recommendations. Some may have minimal implementation requirements and costs; others might require additional funding.

Relevant Strategic Plan Goals and Operational Plan Objectives

The attached report supports Goal III, Modernization of Management and Administration, as it works to ensure the safety and security of court. (Goal III.A.5.)

Attachment

1. Attachment A: Roster of Court Emergency Response and Security Task Force members
2. Attachment B: *Court Emergency Response and Security Task Force: Final Report*

Court Emergency Response and Security Task Force

Appointed August 15, 2007

Hon. Frederick Paul Horn, Chair
Judge of the Superior Court of California,
County of Orange

Mr. Michael M. Roddy
Court Executive Officer
Superior Court of California,
County of San Diego

Hon. Richard D. Aldrich
Associate Justice of the Court of Appeal,
Second Appellate District, Division Three

Mr. Michael Yerly
Clerk/Administrator
Court of Appeal, Sixth Appellate District

Hon. Patricia Bamattre-Manoukian
Associate Justice of the Court of Appeal,
Sixth Appellate District

GOVERNING COMMITTEE OF THE CJER LIAISON

Hon. James R. Brandlin
Judge of the Superior Court of California,
County of Los Angeles

Hon. Arthur A. Wick
Judge of the Superior Court of California,
County of Sonoma

Ms. Donna Hanover
Executive Officer
Superior Court of California,
County of Trinity
[Resigned effective January 2010.]

OFFICE OF GOVERNMENTAL AFFAIRS LIAISON

Ms. Donna Hershkowitz
Acting Director
Office of Governmental Affairs
Administrative Office of the Courts

Hon. Steven E. Jahr (Ret.)
Superior Court of California,
County of Shasta
[Resigned effective October 1, 2012.]

LEGAL SERVICES OFFICE LIAISON

Mr. Michael I. Giden
Attorney
Legal Services Office
Administrative Office of the Courts

Hon. Thomas M. Maddock
Judge of the Superior Court of California,
County of Contra Costa

AOC LEAD TASK FORCE STAFF

Mr. Frederick K. Ohlrich
Clerk of the California Supreme Court
[Resigned effective May 2012.]

Mr. Malcolm Franklin
Senior Manager
Office of Security
Administrative Office of the Courts

Court Emergency Response and Security Task Force: Final Report

DECEMBER 14, 2012



CONTENTS

I. Executive Summary	1
II. Background	4
A. Establishment of the Task Force.....	4
B. The Task Force Begins its Work.....	4
C. Court Security Realignment	6
D. The Strategic Evaluation Committee Report and AOC Restructuring	9
III. Recommendations	11
Recommendation 1— Maintain the AOC Office of Security Because the Necessary and Vital Safety Functions of the Office are Best Coordinated and Implemented Under the Expertise of a Separate Office to Assure the Safety of the Public, Judicial Officers, and Court Employees.	11
Recommendation 2— Establish a Court Security Advisory Committee to Oversee the AOC Office of Security and to Advise the Judicial Council on Court Security and Emergency Planning.....	19
Recommendation 3— Establish a Branchwide Threat and Incident Program to Enhance the Protection of Judicial Officers, Judicial Branch Staff, and the Public.	23
Recommendation 4— Continue to Review and Evaluate the Viability and Usefulness of Establishing Branchwide Security Classification and Staffing Guidelines to Enhance the Safety of California's Courts.	29
Recommendation 5— Continue to Review and Evaluate the Court Security Plan Process to Facilitate and Increase Trial Court Compliance to Ensure that Courts Establish and Keep Current All Necessary Procedures to Protect Every Person Entering the Courthouse.	31
Recommendation 6— Further Develop Court Emergency Planning Tools and Increase Associated Educational Efforts about the Tools to Provide Safe and Accessible Courthouses.....	34

ATTACHMENTS

- A. Final Report Submitted by the National Center for State Courts, with Appendices, dated March 2012
- B. Letter from Judge Frederick Paul Horn, Chair of the Court Emergency Response and Security Task Force, to Justice Douglas P. Miller, Chair of the Executive and Planning Committee, dated June 5, 2012
- C. Excerpt of Report of the Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch, dated November 4, 2011
- D. E-mail from Chief John Muffler, Administrator of the National Center for Judicial Security, United States Marshals Service, to Judge James R. Brandlin, dated June 4, 2012
- E. Summary of Advisory Groups by the Court Emergency Response and Security Task Force's Subcommittee on Security, Standards, Facilities, and Education, dated June 12, 2009
- F. Summary of AOC Office of Security Survey of California Judges and Justices Concerning Threats Received Between December 2005 and December 2006, dated 2007
- G. California Highway Patrol Judicial Protection Section's Information Control Report Form, dated May 2005
- H. California Highway Patrol's Standard Form "STD. 99" (Report of Crime/Incident on State Property), dated March 2010

I. Executive Summary

Unlike virtually any other institution in our society, the judicial branch has the authority to compel citizens to attend court involuntarily, as jurors, witnesses, or parties in connection with civil, family, criminal, dependency, or other pending cases. The task force submits that with this authority comes a moral responsibility to provide a civilized environment uncorrupted by threats and avoidable risks to those who enter the courthouse. Assuring the security of the public who enter California's courthouses, as well as the judges and court employees who serve the public, is necessary to achieve the fundamental judicial branch goal of providing equal access to justice for all Californians. "Courthouses must be a safe harbor to which members of the public come to resolve disputes that often are volatile. Once courthouses themselves are perceived as dangerous, the integrity and efficacy of the entire judicial process is in jeopardy."¹ Court security is, therefore, an *essential* component of judicial administration.

Recognizing the significance of security to judges, court employees, and the public they serve, Chief Justice Ronald M. George (Ret.) established the Court Emergency Response and Security Task Force. He charged the task force with evaluating court security, including emergency planning, continuity of operations, and personal security issues, and with developing recommendations for the Judicial Council to manage, maintain, and enhance security in the courts. Based upon its investigation and collective experience, the task force makes the following recommendations, each of which is discussed at greater length in a separate section of the report.

Recommendation 1—

Maintain the AOC Office of Security Because the Necessary and Vital Safety Functions of the Office are Best Coordinated and Implemented Under the Expertise of a Separate Office to Assure the Safety of the Public, Judicial Officers, and Court Employees.²

The task force recommends that the AOC Office of Security be maintained as a separate office within the AOC Judicial and Court Operations Services Division. Most of the necessary and vital functions performed by the AOC Office of Security require specialized training and experience and cannot be performed effectively by administrative staff or personnel untrained in judicial security and law enforcement techniques. These safety functions are best coordinated and implemented by a separate office under the direction of an experienced professional. Maintaining a separate office will demonstrate the judicial branch's commitment to the safety and security of the public, judicial officers, and court employees and will support equal access to justice throughout the state.

¹ Chief Justice Ronald M. George (Ret.), *State of the Judiciary*, March 15, 2005.

² Effective October 1, 2012, the name of the "Office of Emergency Response and Security" was changed to the "Office of Security." The current name will be used throughout the report.

Recommendation 2—

Establish a Court Security Advisory Committee to Oversee the AOC Office of Security and to Advise the Judicial Council on Court Security and Emergency Planning.

The task force recommends that a standing advisory committee (Court Security Advisory Committee) be established to oversee the AOC Office of Security and to advise the Judicial Council on issues related to court security and emergency planning. Oversight of the AOC Office of Security is necessary to ensure accountability and transparency. Court security is a fundamental area of court administration, necessary to the provision of justice in California, and no current group advises the Judicial Council in this area comprehensively from a branchwide perspective.

Recommendation 3—

Establish a Branchwide Threat and Incident Reporting Program to Enhance the Protection of Judicial Officers, Judicial Branch Staff, and the Public.

The task force recommends that the Judicial Council establish a branchwide threat and incident reporting program to enhance the protection of judicial officers, judicial branch staff, and the public. Statewide documentation of threats and incidents directed to judges and courthouses is necessary to document and allocate the resources needed statewide for court security.

Recommendation 4—

Continue to Review and Evaluate the Viability and Usefulness of Branchwide Security Staffing and Service Guidelines to Enhance the Safety of California's Courts.

The task force recommends that the Judicial Council direct the proposed Court Security Advisory Committee to continue reviewing and evaluating the viability and usefulness of developing and establishing court security classification and staffing guidelines to enhance the safety of California's courts and make recommendations to the Judicial Council as appropriate.

Recommendation 5—

Continue to Review and Evaluate the Court Security Plan Process to Facilitate and Increase Trial Court Compliance and to Ensure that Courts Establish and Keep Current All Necessary Procedures to Protect Every Person Entering a Courthouse.

The task force recommends that the Judicial Council charge the proposed Court Security Advisory Committee with responsibility for continuing to review and evaluate the process for preparing and submitting court security plans, and making recommendations to the council to facilitate and increase trial court compliance with Government Code section 69925. Preparation and maintenance of court security plans ensure that the court and sheriff or marshal establish and keep current all necessary protocols and procedures to best protect every person who enters a courthouse.

**Recommendation 6—
Further Develop Court Emergency Planning Tools and Increase Educational
Efforts about the Tools Because Emergency Planning is Necessary to Provide
Safe and Accessible Courthouses.**

The task force recommends that the Judicial Council direct the AOC Office of Security to (1) disseminate information to educate judges and judicial branch staff about the emergency planning tools, programs, and assistance that it makes available to the courts; (2) further develop the emergency planning tools; and (3) allocate to the AOC the resources to implement this direction because emergency planning is necessary to provide safe and accessible courthouses.

The task force urges the council to adopt these recommendations and provide sufficient funding to implement them because court security is imperative to assure the safety of our courthouses and to provide equal access to justice in California.

II. Background

A. Establishment of the Task Force

Chief Justice Ronald M. George (Ret.) established the Judicial Council's Court Emergency Response and Security Task Force, effective August 15, 2007, appointing Judge Frederick Paul Horn as its chair. In forming the task force, the Chief Justice brought together representatives from existing statewide advisory groups that had been formed to address security and emergency planning in the trial and appellate courts.

The charge of the task force requires it to:

- Evaluate emergency planning, continuity of operations, court security, and personal security issues and develop recommendations for the Judicial Council to manage, maintain, and improve security in the courts through statewide systems and progressive initiatives to increase efficiency, effectiveness, and cost-saving measures in California;
- Provide an interim report to the Judicial Council after 18 months; and
- Provide a final report of recommendations to the Judicial Council at the end of its term.

The task force was originally scheduled to complete its work and report to the council by August 2010; that deadline was extended first to December 2011, and then to June 2012.

B. The Task Force Begins its Work

In November 2007, the chair established two subcommittees, each composed of members of the task force. The Subcommittee on Threat Assessment and Emergency Planning (TAEP) planned surveys of the trial courts on the status of emergency planning and threat management. The Subcommittee on Security, Standards, Facilities, and Education (SSFE) planned examinations of various advisory groups and staff devoted to issues of court security and emergency planning, to investigate and to assess the status of work in four areas: (1) security for judicial officers, (2) security standards for court operations, (3) security issues related to facilities, and (4) training and education. Concurrently with the work of the two subcommittees, the task force began to study how court security is delivered in other jurisdictions, focusing on the State of New York and the federal courts.

In 2009, SSFE and TAEP reported back to the task force on the results of their respective investigations.

TAEP reported on the two surveys it had conducted.

- With respect to the threat management survey, TAEP reported that all 58 trial courts responded. 42 courts contacted their sheriff or marshal to report threats made to judicial officers, court employees, or court property. TAEP reported that only 12 percent of the trial courts report to the California Highway Patrol any threats against judicial officers, as required by Penal Code section 76(b). TAEP observed that there was no common statewide database for threats to courts. Some survey respondents suggested that standardized reporting through the AOC and sharing of information over jurisdictional boundaries would be helpful.³
- With respect to the emergency planning survey, TAEP reported that 57 of the 58 trial courts responded. 25 courts reported having an emergency plan, most of which had been updated within the previous year. 20 courts reported having a continuity of operations plan. Many courts were in the process of preparing plans with the assistance of the AOC Office of Security.

SSFE reported in detail on the charges and work of each of the five advisory groups on court security and on the work of four AOC divisions that focus on court security.⁴ The five advisory groups are discussed at greater length in Recommendation 2, below. SSFE also reported on the status of advisory group and staff work on (1) security for judicial officers; (2) security standards for court operations; (3) security issues related to courthouse facilities; and (4) training and education related to judicial officer and courtroom security. SSFE observed that the guidelines for court security related primarily to funding, but that there was a strong need to develop standards for staffing or services. SSFE noted an ongoing need to ensure that there is no duplication of effort by the various entities working on court security and to assure that all important work is addressed.

Also in 2009, the task force concluded its study of the New York State and federal judiciary models for providing court security.

- In the State of New York, the state-funded courts are transitioning from contracting with local sheriffs to using court-employed security officers. The state supports an academy for training court officers. Initially, there was some resistance to this transition from county law enforcement, but that resistance has diminished over time. In 2008, 45 out of 62 state-funded trial courts provided their own security by employing uniformed court officers. For the remaining 17 state-funded courts, the State of New York contracted with the sheriff or local policy agency. Justice courts, which are funded by the local town or village, rely on locally provided security, if any is provided.

³ Since TAEP conducted its survey, compliance has improved, as documented in Recommendation 5, below.

⁴ These included: (1) the AOC Office of Security; (2) the Office of Court Construction and Management, since October 1, 2012, divided into the Judicial Branch Capital Program Office and the Office of Real Estate and Facilities Management; (3) the Education Division/Center for Judicial Education and Research, known since October 1, 2012, as the Office of Education/Center for Judicial Education and Research; and (4) the Information Services Division, known since October 1, 2012, as the Information and Technology Services Office.

- The United States Marshals Service (USMS) is responsible for a broad range of federal law enforcement responsibilities. Among these are its responsibilities for protecting the federal judiciary and federal courthouses. There is a local district office of the USMS located in each of the 94 judicial districts of the federal court system. The USMS employs a national network of deputy U.S. Marshals, physical security specialists, intelligence analysts, and support staff. They are responsible for the personal security of federal judges and ensuring the safe and secure conduct of judicial proceedings at more than 400 locations. The USMS assesses, mitigates and deters approximately 1,400 threats and inappropriate communications against the judiciary each year. Deputy Marshals handle in-custody defendants and are the overall security of the courthouse facilities, staff, and judges. Court Security Officers (CSOs) are highly trained contract security staff under the supervision of the USMS, who are responsible primarily for facility screening, and building protection systems.

At its June 9, 2010, meeting, the task force concluded that in order to complete its work and make well-supported recommendations to the Judicial Council regarding court security in California with an eye toward branchwide security systems, it needed the assistance of judicial administration professionals who could advise it based on a familiarity with the practice in courts in other jurisdictions within the United States. To perform this work, the AOC contracted with the National Center for State Courts (NCSC) to conduct a study of four areas:

1. Models for providing court security in an economical and efficient manner.
2. Development of a threat/incident reporting system for the California courts.
3. Standards and classifications for court security staffing.
4. Methods for increasing trial court compliance with the timely submission of court security plans under Government Code section 69925.

The task force met with staff from the NCSC to discuss this scope of work at a meeting on August 31, 2010, and the NCSC began its work shortly thereafter. A copy of the final report, submitted by the NCSC, dated March 2012 (NCSC Report), is Attachment “A” to this report.

C. Court Security Realignment

In 2011, events occurred that would have a significant impact on the work of the task force. On January 10, 2011, Governor Brown introduced his proposed budget for fiscal year 2011–2012. In that budget, the Governor proposed a major shift in the state-local relationship by reversing the trend of consolidating control and budget authority in Sacramento. This shift, which the Governor called “realignment,” involved transferring from the state to local government responsibility for providing certain government services and the funding to provide those services. One part of the realignment addressed court security.

The requirement that the sheriffs provide security services to the superior courts dates to the 19th century. In 1883, California law required a sheriff to “[a]ttend all Courts, except Justices’

and Police Courts, held within his county, and obey their lawful orders and directions.”⁵ At that time, trial courts, like the sheriff, were funded by their respective counties, so it was expected that a county officer would provide security for the superior courts in the same way the county provided facilities, employees, and operating funds for the superior courts.

A significant development that impacted the sheriffs’ mandate to provide security to the superior courts was the shift to state funding of the trial courts, known as “trial court funding.” The evolution of trial court funding occurred through legislation enacted from the mid-1980s to the late 1990s. Before 1988, counties were primarily responsible for paying for court operations.⁶ But in the 1980s, the Legislature began to recognize that funding of the trial courts was most logically a function of the state; it saw that counties were increasingly unable to meet the funding requirements of the trial courts such that the quality and timeliness of justice were threatened in some counties.⁷ The state began assuming a greater portion of the burden of funding trial courts with enactment of the Brown-Presley Trial Court Funding Act (Brown-Presley Act) in 1988.⁸ Nine years after passage of the Brown-Presley Act, the state assumed almost complete responsibility for funding trial court operations under the Lockyer-Isenberg Trial Court Funding Act of 1997 (Lockyer-Isenberg Act).⁹

Despite the shift in responsibility from the county to the state for funding court operations, the sheriff continued in most counties to provide court security services to the superior courts. The responsibility of the sheriff to provide these services to the superior courts—and the responsibility of the state-funded superior courts to pay the county for those services—was codified first in Assembly Bill 92¹⁰ and later Senate Bill 1396.¹¹ The latter act, known as the “Superior Court Law Enforcement Act of 2002,” was still the operative statutory framework for the sheriff providing security services to the superior courts when Governor Brown proposed a realignment of court security. By fiscal year 2010–2011, the annual appropriation to the judicial branch for trial court security was a little over \$500 million, most of which superior courts paid to sheriffs subject to the terms of memoranda of understanding.

⁵ Stats. 1883, ch. 75, § 93, p. 320. That language is currently found in modified form in Government Code section 69921:

Except as otherwise provided by law, whenever required, **the sheriff shall attend all superior court [sessions] held within his or her county.** A sheriff shall attend a noncriminal, nondelinquency action, however, only if the presiding judge or his or her designee makes a determination that the attendance of the sheriff at that action is necessary for reasons of public safety. . . . The sheriff shall obey all lawful orders and directions of all courts held within his or her county. [Bold added.]

⁶ In the 1982–1983 fiscal year, for example, the state contributed approximately 11 percent to the funding of the trial costs, with the counties bearing the rest. (Judicial Council of Cal., 1983 Report to the Governor and the Legislature, part 1, chapter 8, Trial Court Costs and Revenue, pp. 35, 41, and 43.)

⁷ Stats. 1997, ch. 850, § 2(a) & (f).

⁸ Stats. 1988, chs. 944 & 945.

⁹ Assem. Bill 233; Stats. 1997, ch. 850.

¹⁰ Stats. 1998, ch. 764.

¹¹ Stats. 2002, ch. 1010.

Governor Brown proposed to reduce funding to the superior courts by approximately \$500 million, increase the amount of funding to the counties by that amount, and transfer responsibility for court security expenses from the superior courts to the counties. In 2011, the Legislature passed two bills that implement this proposal. Assembly Bill 118¹² established in the state treasury a Trial Court Security Account in the Local Revenue Fund 2011, which is funded with specified revenues.¹³ The money in the account is continuously appropriated and allocated to individual counties. Counties must deposit that money into a county-established Trial Court Security Account in the county treasury and may use the money in the account only to fund trial court security provided by sheriffs.¹⁴ Assembly Bill 121,¹⁵ a bill to amend the Budget Act of 2011, authorized the Director of Finance to reduce the appropriation to the Trial Court Trust Fund, to reflect any funding for court security provided directly to counties.

The Governor approved both AB 118 and AB 121 on June 30, 2011, and the realignment of court security went into effect for fiscal year 2011–2012.¹⁶ A year later, effective June 27, 2012, the Superior Court Law Enforcement Act of 2002 was amended to reflect the changes resulting from the realignment of court security and was renamed the Superior Court Security Act of 2012.¹⁷ The new law still requires the presiding judge of a trial court, in conjunction with the sheriff or marshal, to prepare a court security plan¹⁸ and requires the court and sheriff to enter into a memorandum of understanding,¹⁹ however it repealed the provisions that defined the allowable costs that a court could pay to the sheriff.²⁰

Although realignment was not intended to fundamentally affect the provision of security services to the superior courts, by changing the funding structure, realignment has taken away from the superior courts much of the leverage superior courts had in negotiating the cost, and therefore the scope, of these services. In meetings with the administration, AOC staff have urged the adoption of statewide service and staffing standards or guidelines to assure that the scope of services to the superior courts is not reduced as a result of realignment. These efforts have been unsuccessful because the administration is concerned that imposing classification or staffing standards or guidelines would, to the extent they imposed new costs on the sheriffs, constitute an unfunded mandate under article XIII B, section 6 of the California Constitution.

¹² Stats. 2011, ch. 40.

¹³ Gov. Code, § 30025.

¹⁴ Gov. Code, § 30025(f)(3).

¹⁵ Stats. 2011, ch. 41, § 2.

¹⁶ Realignment did not affect any expenses that the court paid directly to a party other than the sheriff. Thus, the two courts that employ marshals (the Superior Courts of Shasta and Trinity Counties) continue to do so with funds allocated from the Judicial Council and under the direct oversight of the court. Likewise, courts that paid private security vendors for screening services continue to do so with funds allocated from the Judicial Council. The appellate courts also were unaffected by the court security realignment.

¹⁷ Sen. Bill 1021 (Stats. 2012, ch. 41, §§ 26–36).

¹⁸ Gov. Code, § 69925.

¹⁹ Gov. Code, § 69926(b).

²⁰ Sen. Bill 1021 (Stats. 2012, ch. 41, § 36).

The changes brought about by realignment have had a significant impact on the work of the task force. The task force requested an extension of time to submit its final report to the council so that the task force could examine the impact of realignment and determine how realignment affected the recommendations it had been working on during its tenure. The role of the Judicial Council and the superior courts in governing court security has become more limited than it was. This has had an impact on the scope of the recommendations the task force can make. For example, the task force considered recommending service and staffing guidelines to assure a minimum level of court security statewide and it requested advice from the NCSC on this topic. Following realignment, however, the Judicial Council does not have the ability to enforce such guidelines, because it does not have authority over funding. The task force believes that it is important to document the work that it did, even if a recommendation is not viable at present. The funding and governance of court security may change at some time in the future and the deliberations of the task force may be of value to those working on court security in the future.

D. The Strategic Evaluation Committee Report and AOC Restructuring

The task force had completed an almost final draft of its report by May 2012. One more event occurred that month, which changed the course of the task force's report yet again: The Strategic Evaluation Committee (SEC) issued its final report on May 24, 2012.²¹ Chief Justice Tani G. Cantil-Sakauye, had established the SEC in March 2011, appointing 14 judges and four advisory members.²² She asked the committee to conduct an in-depth review of the AOC, with a view toward promoting transparency, accountability, and efficiency.²³

The SEC devoted four pages of its report to the AOC Office of Security,²⁴ and made three recommendations concerning the office. Specifically, the SEC recommended:

Recommendation No. 7-54: There is no need for a stand-alone Office of Emergency Response and Security. Most necessary functions performed by the office can be reassigned and absorbed by existing units in the Judicial and Court Operations Services Division.

Recommendation No. 7-55: The functions of this office should be refocused and limited to those reasonably required by statute or by the Rules of Court, primarily including review of security plans for new and existing facilities; review of court security equipment, if requested by the courts; and review of emergency plans.

Recommendation No. 7-56: Reductions in this office are feasible. The office cannot effectively provide branch-wide judicial security and online protection for

²¹ SEC Report, accepted by Judicial Council of Cal., June 21, 2012 (SEC Report). A copy of the SEC Report is available at www.courts.ca.gov/documents/SEC_Final_Report_May_2012_withcoverletter.pdf.

²² Judicial Council of Cal. News Rel., dated Mar. 29, 2011. The news release is available at www.courts.ca.gov/18260.htm.

²³ SEC Report, p. 1.

²⁴ *Id.* at pp. 144–147.

all judicial officers. Positions allocated for such functions should be eliminated. The Administrative Director should evaluate whether some activities undertaken by this office are cost effective, such as judicial security and online protection functions.

The task force met on June 5, 2012, and decided to take immediate action to respond to the recommendations in the SEC Report. The members of the task force drafted a letter for Judge Horn's signature to be delivered to Justice Douglas P. Miller, in his capacity as chair of the Judicial Council's Executive and Planning Committee. The letter explained the history of the task force and provided some preliminary information about the importance of court security to judicial administration. The letter expressed support for the work of the SEC, but also provided information that supported maintaining a separate office for court security within the AOC, among other topics. A copy of the letter is Attachment "B." Justice Miller and Judge Horn agreed that the task force would postpone submitting its final report, pending more information on the Judicial Council's consideration of the SEC Report.

At its August 31, 2012 meeting, the Judicial Council took two actions that affected the AOC Office of Security. First, the Judicial Council adopted recommendations to realign the AOC's organizational structure that were presented by Judge Steven Jahr, then-incoming Administrative Director of the Courts, and Jody Patel, then-Interim Administrative Director of the Courts.²⁵ That recommendation changed the name of the "Office of Emergency Response and Security" to the "Office of Security" and moved the office from the former Executive Office to the newly established Judicial and Court Operations Services Division. Second, the Judicial Council adopted the Executive and Planning Committee's recommendations regarding the SEC Report. With respect to the recommendations on the AOC Office of Security, the council directed the Administrative Director of the Courts "to return to the Judicial Council with an analysis, defining the necessary emergency response and security functions for the branch and a recommendation on the organizational plan for council approval."²⁶ That recommendation is due to the Judicial Council at its December 14, 2012 meeting.²⁷

Judge Jahr (a member of the task force until he resigned following his appointment as Administrative Director of the Courts) requested that the task force complete its report and submit it to the Judicial Council at its December 14, 2012 meeting to coincide with the submission of his recommendation regarding the AOC Office of Security. This will permit the Judicial Council to have the full benefit of the task force's expertise and its extensive work on court security when it assesses the future of the AOC Office of Security.

²⁵ Minutes of Judicial Council of Cal. Meeting, Aug. 31, 2012, p. 11.

²⁶ *Id.* at p. 11, attachment 3, p. 52.

²⁷ *Ibid.*

III. Recommendations

Recommendation 1—

Maintain the AOC Office of Security Because the Necessary and Vital Safety Functions of the Office are Best Coordinated and Implemented Under the Expertise of a Separate Office to Assure the Safety of the Public, Judicial Officers, and Court Employees.

The task force recommends that the AOC Office of Security be maintained as a separate office within the AOC Judicial and Court Operations Services Division. Most of the necessary and vital functions performed by the AOC Office of Security require specialized training and experience and cannot be performed effectively by administrative staff or personnel untrained in judicial security and law enforcement techniques. These safety functions are best coordinated and implemented by a separate office under the direction of an experienced professional. Maintaining a separate office will demonstrate the judicial branch's commitment to the safety and security of the public, judicial officers, and court employees and will support equal access to justice throughout the state.

Rationale for Recommendation

The AOC Office of Security was established as a unit within the Executive Office in 2005. The work of the AOC Office of Security currently falls into three broad areas:

- Personal Security
- Physical Security
- Emergency Planning

These three areas, and the AOC Office of Security's services in each, are summarized in the sections below. A more complete list of the functions performed by the AOC Office of Security as of 2011, as well as the funding for the office, was included in the November 4, 2011 report of the Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch. A copy of the portion of the report devoted to the AOC Office of Security is Attachment "C."

The SEC suggests that these safety functions "can be reassigned and absorbed by existing units in the Judicial and Court Operations Services Division."²⁸ The task force respectfully disagrees. Only a separate office of trained professionals dedicated to court security and emergency response planning is consistent with the best practices for courthouse and judicial safety. In an e-mail, dated June 4, 2012, to task force member Judge James Brandlin, from Chief John Muffler, Administrator of the National Center for Judicial Security, United States Marshals Service of the United States Marshals Service (USMS), a national leader in courthouse security and judicial protection, noted that:

²⁸ SEC Report, pp. 144–147.

Trained, professional personnel with expertise in risk management, protective investigations and emergency preparedness are essential to sustaining our rule of law in the United States. Protecting judges, legislators and public safety officials is an inherent part of our democracy and ensures our system of justice is fair and impartial. Untrained individuals in these disciplines would not be able to provide the required level of protection rightly needed. The United States Marshals Service provides protective details to threatened officials after careful examination of the threat information. Security details are maintained until the threat is mitigated by operational and administrative professionals in law enforcement and intelligence, respectively. At no time is untrained staff—or non-Marshals Service employees—part of this mitigation process; nor should it be left to untrained individuals to make a life or death call on a threat or to evaluate risk.

A copy of the e-mail from which this quote is taken is Attachment “D.” Consistent with the principles outlined by Chief Muffler, the vital and necessary safety functions performed by the AOC Office of Security should not be distributed to vendors or to untrained staff in other offices of the AOC.

A. Personal Security Programs and Services

A primary function of the AOC Office of Security is to provide programs and services to support the personal security of judicial officers and judicial branch staff. The major programs and their significance are summarized below.

Judicial Privacy Protection Opt-Out Program

In the highly specialized world of dignitary protection and threat assessment, experts agree that privacy protection, namely the ability to “hide in plain sight,” is the first line of defense for judicial officers. Judicial threat assessment studies undertaken by the USMS and others make it clear that judges are most vulnerable away from the courthouses where their security provider is located.²⁹ One of the collateral impacts of an effective entry weapons screening program is that it forces potential stalkers and attackers to focus their efforts to attack judges away from the courthouse. However, when a judge leaves the building, he or she is not normally assigned a protective detail. It is beyond dispute that judges are most vulnerable at home.³⁰

In the Internet age, obtaining home address information online can be very easy *if* the judge does not take early affirmative steps to block or mask that information. Many of the solved cases in the last several decades wherein suspects have stalked, harassed, or killed a judge involve

²⁹ In the last century, 34 judges were killed by nonfamily members, 13 were killed at the courthouse (most of which were killed before weapon screening procedures were instituted), another 21 were killed away from the courthouse. Of the judges killed away from the courthouse, 10 were killed in transit and 11 were killed at home. In addition, four spouses were also killed. (Baker, *Murdered Judges of the Twentieth Century* (2003).) See also, the discussion in Recommendation 3, below.

³⁰ *Ibid.*

preplanning and research on the part of the suspect, primarily through Internet searches and public records checks and *not* by physically following the target, which would expose the stalker to potential detection. Therefore, protecting home address information has become critical to improving a judge's safety. The California Legislature has specifically recognized that danger and provided California public safety officials with home address privacy protection tools not generally available to other members of the public.³¹

There are many websites that sell personal information about individuals or provide it for free. Online data vendors gather this information from several sources including other data vendors, directory listings like telephone books, and public records. Thus, in 2005, the AOC Office of Security collaborated with the California Office of Privacy Protection³² and the California Attorney General's Office on a program to protect judges' on-line privacy. On behalf of those judicial officers that participate, the AOC Office of Security makes a formal request under Government Code section 6254.21 (an "opt-out demand") to have the judicial officer's home address and phone number removed from up to 15 major online data vendor websites that sell or share such information with others.

The SEC Report suggests that the tasks related to removing personal information from websites "may be best left to local courts or to judicial officers themselves," citing a recent California Judges Association arrangement with a private vendor to submit opt-out demands of Internet data vendors for an annual fee.³³

The task force respectfully disagrees with the SEC's suggestion. Assigning the responsibility to the individual judges creates a serious safety issue. Not all judges have the technological skill or time to do it. Even for those who do, it is a poor use of valuable judicial resources. This task is more efficiently and effectively performed by one staff person in the AOC Office of Security, than by individual judges whose limited time is better spent on the critical judicial functions that only they can perform.

Using the AOC Office of Security to perform this function is vastly preferable to hiring an outside vendor or having each court bear this responsibility for the following reasons:

- The release of an outsourced list of home addresses and telephone numbers of all of our judicial officers should never be entrusted to a private vendor who has not undergone a law enforcement background check. Even if the judicial branch could arrange for background checks of the vendor's employees, it would have to constantly monitor those vendors. This is more expensive, if not impossible, to do effectively. It is more efficient to entrust the task to one, background-checked employee of the AOC Office of Security.

³¹ See Gov. Code, §§ 6254.21, 6254.24; Elec. Code, § 2166.7; Veh. Code, §§ 1808.2, 1808.4, 1808.6.

³² Then part of the California Department of Consumer Affairs' Office of Information Security and Privacy Protection. The office has since become the Privacy Enforcement and Protection Unit of the Office of the Attorney General.

³³ SEC Report, p. 146.

- The information released to the vendor will have to be kept current, which will require repeated transfers to the vendor of this sensitive information, multiplying the risk of its misuse. The loss of this information could be disastrous breach of safety for the judicial branch.
- The cost of hiring an outside vendor to make the opt-out demands is more expensive. The current cost for most private online privacy protection services is more than \$100 per person. Over 2,000 judicial officers and approximately 3,400 additional family members have participated in the AOC Office of Security program. The expense in outsourcing this task would be much more costly than doing it in house.
- Having one trusted, background-checked employee of the AOC Office of Security handling all statewide judicial opt-out demands is much more effective and cost-efficient than training 58 superior court staff members or over 2,000 judicial officers to perform the same tasks.
- The AOC Office of Security uses the updated current national list of Internet data vendors published by the California Office of Privacy Protection.³⁴ Many of the private online protection services do not make demands of all of the major Internet data vendors on this list. A judge using a private online opt-out service that does not cover all of the major Internet data vendors would be given a false sense of security and still have significant exposure.

No Internet privacy protection program is perfect. Removing information from the Internet is a challenging, complex, and evolving task. The AOC Office of Security's program is not staffed to address individual opt-out demands outside its scope. However, participation in the program provides a strong foundation for protecting a California judicial officer's privacy and it is the most efficient and cost-effective way to address this fundamental and necessary job.

In addition to operating the program, the AOC Office of Security, in conjunction with other law enforcement and judicial officers, develops and maintains written guidance for judicial officers about privacy protection, and presents a program on privacy protection at the New Judges Orientation.

Contractor Clearance and Badging Program

The AOC Office of Security operates a Contractor Clearance and Badging Program. Under this program, whenever the AOC sends a contractor to a courthouse, if the contractor is going to have access to a secured area of the courthouse in which a California Law Enforcement Telecommunications System (CLETS) terminal or information from CLETS is located, the AOC Office of Security performs a CLETS-compliant background check with the California Department of Justice. Once approved, the contractor receives a badge; the AOC Office of

³⁴ Now, the Privacy Enforcement and Protection Unit of the Office of the Attorney General.

Security retrieves the badge when the contractor is finished with the scope of work or receives notice of a change in status. The AOC Office of Security has conducted 2,100 background checks under this program and actively monitors and maintains over 800 badges.

If the AOC Office of Security did not operate this program, each court that subscribes to CLETS would be required to conduct its own background check, keep the contractor under escort, or be in violation of Department of Justice regulations governing CLETS subscribers. This would impose an additional burden on courts that are already understaffed and focused on providing necessary services to the public. In addition, it would be cumbersome and inefficient. Once the AOC Office of Security has conducted a background check, the contractor can work in any court. If each court had to conduct a background check, the courts would either have to communicate amongst each other, confirm they had continued to monitor the contractor, or conduct separate, redundant background checks.

Personal Security for Judicial Council Events

The AOC Office of Security provides personal protection services at certain Judicial Council events, including Judicial Council meetings and Bench Bar Conferences. Although many judges attend these meetings, the sheriffs, who have primary responsibility for security in the trial courts, do not attend such meetings. The AOC Office of Security is the only office within the AOC that has peace officers on its staff that can provide judicial protection services for Judicial Council events.³⁵ Although it lacks the staff to provide personal protection services for all events, the AOC Office of Security does provide security for the most high-profile meetings.

The task force recommends that the AOC Office of Security continue to operate as a separate office with responsibility for personal protection services at certain Judicial Council events.

Responding to Threats to Judicial Officers

The AOC Office of Security, on request, will assist judicial officers, courts, and local law enforcement when judges receive threats. Personnel from the AOC Office of Security with expertise in responding to threats can assist with evaluating incidents and facilitating communications with law enforcement agencies.

B. Physical Security Programs and Services

The AOC Office of Security provides a number of programs and services that address the security of judicial branch facilities.

³⁵ Security coordinators have limited peace officer status under Penal Code section 830.36(b).

Screening Equipment Replacement Program

The AOC Office of Security administers the Screening Equipment Replacement Program to arrange and pay for the replacement of broken and outdated equipment as well as service agreements on equipment that has been replaced. The AOC Office of Security inventories, evaluates, and tracks hundreds of pieces of screening equipment in the trial courts to determine what equipment needs to be replaced. The program is funded from the Trial Court Trust Fund and each court's participation in the program is voluntary. The program negotiates statewide master contracts that take advantage of the bargaining power of the largest state court system in the country. These agreements result in better price and service terms than many courts could achieve if they were negotiating separately. The facilities programs rarely pay for such equipment, as they focus on the use of facilities funding for construction and maintenance issues, not equipment. In addition, the Office of Security has developed expertise regarding radiation and code compliance to assist and advise the trial courts on this security equipment. This enhances the safety of courthouses for judicial officers, court employees, and the public.

Court Security Grant Program

The AOC Office of Security administers a grant program to fund enhancements to insufficient security systems in trial court facilities, including site assessment, scope/installation details, work oversight and inspection, and maintenance for duress alarms, access systems, video surveillance systems, and other equipment. The program was previously funded from the Trial Court Improvement Fund and is now funded from the Trial Court Improvement and Modernization Fund. In support of this program, the AOC Office of Security has negotiated statewide master agreements. These agreements provide better price and service terms than many courts could achieve if they were negotiating separately.

Court Security Plans

Under Government Code section 69925, the presiding judge of a trial court, in conjunction with the sheriff or marshal, must develop a court security plan. Trial courts must submit the plans to the AOC,³⁶ and the AOC is responsible for reviewing the plans for completeness.³⁷ The AOC Office of Security has performed this function since 2009, when plans were first submitted. No other office within the AOC has the expertise in security sufficient to review these plans—or to assist the courts in preparing a court security plan. The AOC Office of Security developed an online interactive security plan template, which assists courts in preparing court security plans. In addition, AOC Office of Security staff will, at the request of a court, make themselves available to assist courts individually. Court security plans are discussed at greater length under Recommendation 5.

Court Security Assessments and Consulting

At the request of a court, the AOC Office of Security will provide on-site security assessments and other guidance based on the personnel's subject matter expertise. The AOC Office of

³⁶ Cal. Rules of Court, rule 10.172(d).

³⁷ Cal. Rules of Court, rule 10.172(e).

Security also provides consultation services to courts and other AOC offices concerning the security aspects of facilities maintenance and construction. The SEC Report notes that there “is value in the [AOC Office of Security’s] review of court construction projects in order that necessary security considerations are included in new construction projects.”³⁸

If the AOC Office of Security did not provide these services, courts would have to go without them, or pay a vendor, such as the National Center for State Courts. The services provided by the AOC Office of Security are more cost-effective and are provided by staff with California-specific training and experience.

C. Emergency Response Programs and Services

The AOC Office of Security takes the lead in emergency planning activities for the judicial branch. This is manifest in two primary programs.

Continuity of Operations Planning

The Federal Emergency Management Agency (FEMA) defines a Continuity of Operations Plan (COOP) as an internal effort within individual components of a government to ensure the capability exists to continue essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

In 2007, the AOC Office of Security purchased a web-based tool that guides courts through the process of preparing a COOP, generates a plan, including all necessary information, securely preserves it, and makes it accessible on fully redundant sites located out of state. The AOC Office of Security offers training and access to the tool, at no cost, to all courts.

Emergency Response Planning

In contrast to COOPs, which are designed to facilitate a court continuing all essential functions within 12 hours of an emergency and sustaining those functions for up to 30 days, an Emergency Response Plan is intended to address the court’s response in the first 72 hours following an emergency. In 2009, the AOC Office of Security made available to the courts an Emergency Response Plan tool, available as a module of the COOP tool and purchased from the same vendor. As with the COOP tool, the AOC Office of Security offers training and access to the tool, at no cost, to all courts.

³⁸ SEC Report, p. 146. Although this conclusion is modified a page later, where the report questions whether AOC Office of Security review is necessary, given that architects and building professionals are charged by contract with integrating security features into a building. The task force believes that the initial conclusion is correct. The safety of courthouses cannot be entrusted solely to third parties; AOC Office of Security review is necessary to verify at an early stage that appropriate security features are properly incorporated into courthouse design.

D. The Task Force Recommends that the Judicial Council Direct the Administrative Director of the Courts to Maintain the Office of Security as a Separate Office and that the Proposed Advisory Committee Review Staffing and Scope of Work for the Office

The AOC Office of Security is currently headed by a Senior Manager who reports to the AOC Chief Operating Officer. Staff include four security coordinators, two analysts, and an administrative secretary. The AOC Office of Security recently lost an analyst due to staff reductions resulting from recent budget cuts. This has limited the services that the office provides on COOPs and emergency planning. The four security coordinators each support the physical and personal security functions. Two are located in the San Francisco office, and one each is located in the Sacramento and Burbank offices, respectively. One analyst staffs the Judicial Privacy Protection Opt-Out Program, and badging and access functions; the other analyst staffs the Screening Equipment Replacement Program and the Security Grant Program. The administrative secretary staffs the Contractor Clearance and Badging Program. Both analysts and the secretary are located in the San Francisco office under the direct supervision of the Senior Manager.

The task force recommends that the Judicial Council direct the Administrative Director of the Courts to maintain the AOC Office of Security as a separate office under the Judicial and Court Operations Services Division. The task force further recommends that the proposed advisory committee review the scope of work, organization, and appropriate staffing for the office and make a recommendation to the Judicial Council regarding any appropriate changes.

In addition, the task force recommends re-naming the “Office of Security” to the “Office of **Court** Security.” The task force agrees with the recent change deleting the words “emergency response” from the name of the office. Although emergency response planning is an important part of the AOC Office of Security’s work, a more concise name, with an emphasis on security, better communicates the AOC Office of Security’s most important function. However, because the AOC Office of Security’s services and programs are directed primarily to supporting the security and emergency response planning for the courts, the task force recommends the word “court” should be included in the name of the office. The task force believes this is consistent with the SEC Report’s emphasis on the AOC’s service to the courts and is also consistent with the practice in other states, as reflected in the NCSC Report.³⁹

³⁹ For example, Oregon established an Office of Court Security (NCSC Report, p. 3-5); the Ohio Supreme Court maintains an Office of State Court Security (*ibid.*); Utah has a State Security Director. (NCSC Report, p. 3-7.)

Recommendation 2—

Establish a Court Security Advisory Committee to Oversee the AOC Office of Security and to Advise the Judicial Council on Court Security and Emergency Planning.

The task force recommends that a standing advisory committee (Court Security Advisory Committee) be established to oversee the AOC Office of Security and to advise the Judicial Council on issues related to court security and emergency planning. Oversight of the AOC Office of Security is necessary to ensure accountability and transparency. Court security is a fundamental area of court administration, necessary to the provision of justice in California, and no current group advises the Judicial Council in this area comprehensively from a branchwide perspective.

Rationale for Recommendation

The SEC's first recommendation, adopted by the Judicial Council,⁴⁰ was a reaffirmation of an important principle:

Recommendation No. 4-1: The Judicial Council must take an active role in overseeing and monitoring the AOC and demanding transparency, accountability, and efficiency in the AOC's operations and practices.

Consistent with its adoption of this principle, the Judicial Council must take an active role in overseeing and monitoring the necessary and vital work of the AOC Office of Security. The Judicial Council relies on its advisory committees to assist it in investigation and fact-finding efforts, and in reviewing and evaluating programs, procedures, and practices. Although the Judicial Council must take ultimate responsibility for overseeing the AOC Office of Security, an advisory committee with expertise in court security could assist the Judicial Council by consulting with and overseeing the AOC Office of Security on a regular basis.

Although court security is one of the most important areas of court administration, there is no advisory committee established to address this area for the entire judicial branch. There are advisory committees on various areas of legal practice and procedure⁴¹ and advisory committees for other significant areas of court administration, including court technology,⁴² but there is no advisory committee for court security for the entire judicial branch.

To assess how the judicial branch addresses issues related to court security and emergency planning and response, and to determine if a different governance structure would be appropriate, in 2009, the task force's Subcommittee on Security, Standards, Facilities, and

⁴⁰ SEC Report, p. 44; Minutes of Judicial Council of Cal. Meeting, Aug. 31, 2012, p. 11.

⁴¹ See Cal. Rules of Court, rules 10.40–10.44, establishing the Appellate, Civil and Small Claims, Criminal Law, Family and Juvenile Law, and Probate and Mental Health Advisory Committees.

⁴² Cal. Rules of Court, rule 10.53 establishes the Court Technology Advisory Committee.

Education (SSFE) completed an inventory of the advisory groups and AOC divisions that work on these issues.

The SSFE identified four advisory groups; the four advisory groups identified by SSFE in 2009 were:

1. The Appellate Court Security Committee
2. The Working Group on Court Security
3. The Working Group on Court Security Fiscal Guidelines
4. The Court Security Education Committee

The SSFE also found that the judicial branch has formed ad hoc committees for limited terms to address specific needs. For example, an ad hoc committee was formed to address proposed legislation related to court security realignment. A detailed summary, including the authority, charge, membership, and reporting duties of each of the different groups, is Attachment “E.”

None of the existing groups sufficiently addresses all court security and emergency response issues throughout the judicial branch. The Appellate Court Security Committee addresses security issues only in the appellate courts. The two working groups address security only in the trial courts and are likely to be disbanded in the near future as a result of court security realignment.⁴³ The Court Security Education Committee was disbanded in 2009. Ad hoc committees are formed for limited terms for very specific purposes.

California Rules of Court, rule 10.34(a) summarizes the duties and responsibilities of advisory committees, generally:

(a) Role

Advisory committees are standing committees created by rule of court or the Chief Justice to make recommendations and offer policy alternatives to the Judicial Council for improving the administration of justice within their designated areas of focus by doing the following:

- (1) Identifying issues and concerns affecting court administration and recommending solutions to the council;

⁴³ Effective June 27, 2012, with the passage of SB 1021, the statutory requirement that the Judicial Council establish the two working groups was repealed. The reason that the requirement was repealed is that the primary function of the two groups—to establish the allowable costs that a court could pay to a sheriff—is no longer needed following the realignment of court security funding. Because the primary function of the groups is no longer needed, the task force understands that the two working groups will likely be disbanded as part of an overall review of all Judicial Council advisory groups. The task force supports dissolving the two working groups because the scope of the groups was not broad enough to encompass the scope of work that an advisory committee would. However, the absence of the working groups provides additional support for the task force’s recommendation that a Court Security Advisory Committee be established.

- (2) Proposing necessary changes to rules, standards, forms, and jury instructions;
- (3) Reviewing pending legislation and making recommendations to the Policy Coordination and Liaison Committee on whether to support or oppose it;
- (4) Recommending new legislation to the council;
- (5) Recommending to the council pilot projects and other programs to evaluate new procedures or practices;
- (6) Acting on assignments referred by the council or an internal committee; and
- (7) Making other appropriate recommendations to the council.

No existing group has this broad a charge for court security in the judicial branch. In recognition of the importance of court security to the administration of justice and to ensure that the council has judicious advice in this area, the task force recommends that the Judicial Council establish a Court Security Advisory Committee. The advisory committee should be charged with performing all the duties and responsibilities identified in rule 10.34 of the California Rules of Court with a focus on court security and emergency planning and response. The membership of the committee should be drawn from within the judicial branch so that the committee can act in the best interests of the public and the entire court system. The committee may consult with entities outside the branch, including sheriffs and counties, as needed. But the focus of the committee should be the needs of the branch.

In addition to the broad charge for court security, the task force also recommends the Judicial Council provide more specific direction, as outlined in the other recommendations. Specifically, the task force recommends that the Judicial Council direct the proposed advisory committee to:

- Recommend a threat and incident reporting program;
- Continue to review and evaluate the viability of statewide security standards;
- Continue to review and evaluate court security plan process;
- Recommend enhancements to court emergency planning tools.

Lastly, the task force recommends that the proposed Court Security Advisory Committee be charged with taking an active and continuous role in overseeing and consulting with the AOC Office of Security. Although the Judicial Council has ultimate responsibility for overseeing the AOC Office of Security, the proposed Court Security Advisory Committee can assist the council by reviewing and evaluating the AOC Office of Security's operations and staffing on a regular basis, and making recommendations to the council, as appropriate. In addition, the proposed Court Security Advisory Committee can be a resource to the AOC Office of Security. AOC staff

frequently find it useful to consult with courts to assist them in their work. The proposed Court Security Advisory Committee will provide a group of judicial officers and court administrators appointed by the Chief Justice that the AOC Office of Security can confer with, as needed.

Although the proposed Court Security Advisory Committee should address the court security and emergency planning needs of the entire branch, the task force has concluded that there is no need to disband or make any changes to the operations of the Appellate Court Security Committee. The appellate courts are in a unique position. The appellate courts are not subject to the court security realignment, because they contract with the California Highway Patrol and private security guards, not local sheriffs. The Appellate Court Security Committee, as currently operated, is adequately meeting the needs of the appellate courts.

Recommendation 3—

Establish a Branchwide Threat and Incident Program to Enhance the Protection of Judicial Officers, Judicial Branch Staff, and the Public.

The task force recommends that the Judicial Council establish a branchwide threat and incident reporting program to enhance the protection of judicial officers, judicial branch staff, and the public. Statewide documentation of threats and incidents directed to judges and courthouses is necessary to document and allocate the resources needed statewide for court security.

Rationale for Recommendation

A. Threats and Incidents Involving Judges and Courts Are Increasing

According to reports and surveys conducted by the federal government, the Center for Judicial and Executive Security (CJES), and the AOC Office of Security, threats and violent incidents involving judges and courts are numerous and of increasing seriousness.

At the federal level, the United States Marshals Service (USMS) reports that the number of judicial threat investigations has almost tripled from 565 cases in fiscal year 2002 to 1,580 cases in fiscal year 2010.⁴⁴ More federal judges were assassinated in the last 30 years than in the previous 175 years.⁴⁵

In 2010, Steven K. Swensen, formerly with the USMS and now director of CJES, prepared a nationwide study (CJES Study) of significant violent incidents that involved state and local judges or courthouses between 1970 through 2009.⁴⁶ The CJES Study lists chronologically 185 significant incidents involving shootings, bombings, and arson attacks directed against state and local judges or courthouses.⁴⁷ During these incidents, 147 individuals were killed,⁴⁸ including 18 judges,⁴⁹ and 107 people were seriously wounded.⁵⁰

In 2007, the AOC Office of Security conducted a survey of California judges and justices concerning threats received between December 2005 and December 2006. The survey revealed a large number of threats: 855 judicial officers reported 296 threats, 72 of which were considered imminent. A summary of the responses to the AOC Office of Security survey is

⁴⁴ NCSC Report, p. 1-1.

⁴⁵ Frederick S. Calhoun, *Hunters and Howlers: Threats and Violence Against Federal Judicial Officials in the United States, 1789–1993* (University of Michigan Library, 1998), p. 107.

⁴⁶ Center for Judicial and Executive Security, *Court-Targeted Acts of Violence: Incidents 1970–2010* (2010).

⁴⁷ The author states that this list is representative, not exhaustive, due to the inconsistency and limitations of the documentation of these incidents. (CJES Study, p. III.)

⁴⁸ CJES Study, p. XV.

⁴⁹ *Ibid.*

⁵⁰ CJES Study, p. XVI.

Attachment “F.” The California Highway Patrol (CHP) also collects data on threats to California judges, their families, and staff, which is discussed at greater length below.

These statistics demonstrate the rising level of criminal activity directed at judges and courts. This increase jeopardizes the administration of justice in California. Court security is necessary to reduce this activity, protect the judiciary, and preserve access to the courts throughout California.

B. A Threat and Incident Program is Important to the Safety of the Judicial Branch

“Physical security countermeasures constitute only half of a complete security program. A sound threat-management process composes the other half. It consists of identifying, assessing, and managing problem individuals, including those of violent intent.”⁵¹ There are four essential elements to any threat and incident program:

1. Reporting of threats and incidents;
2. Assessing, analyzing, and processing the reported data and sharing it with appropriate entities;
3. Managing and responding to the threat or incident; and
4. Providing adequate funding and resources to implement the above three elements.

The task force has reviewed other programs and notes that they integrate all four elements. The USMS provides an integrated program for the federal judiciary and, as discussed below, the CHP provides a similar integrated program for the appellate courts in California.

Because 59 different law enforcement agencies⁵² in the state are responsible for the third element (managing the response to a threat or incident), a fully integrated statewide program is not possible at this time. Threats and incidents are not necessarily limited, however, to a single county, or a specific court. Information on a threat in one court may be relevant to a threat in another court, e.g., when the same individual is making threats in multiple jurisdictions, or when the victim resides in a jurisdiction other than where the threat occurred. A single database of threats and incidents occurring in all courts throughout the state would increase the ability to provide security for judicial officers, court employees, and the public using courthouses.

C. The Current Law and Practice for Threat Reporting Varies within the Judicial Branch

The task force reviewed the current law and practice in California. There are currently two statutes that require reporting: one that addresses threats to persons; the other, incidents occurring on state property. Neither is specific to the judicial branch.

⁵¹ Frederick S. Calhoun and Stephen W. Weston, *Threat Assessment and Management Strategies: Identifying the Howlers and Hunters* (CRC Press, 2009), p. 7.

⁵² Specifically, the CHP provides security for the six Courts of Appeal and the Supreme Court; 56 sheriffs and two marshals provide security for the superior courts.

The first statute is Penal Code section 76, which requires all law enforcement agencies to report to the CHP all threats of death or serious bodily harm to certain public officials, including judges:

(a) Every person who knowingly and willingly threatens the life of, or threatens serious bodily harm to, any elected public official, county public defender, county clerk, exempt appointee of the Governor, judge, or Deputy Commissioner of the Board of Prison Terms, or the staff, immediate family, or immediate family of the staff of any elected public official, county public defender, county clerk, exempt appointee of the Governor, judge, or Deputy Commissioner of the Board of Prison Terms, with the specific intent that the statement is to be taken as a threat, and the apparent ability to carry out that threat by any means, is guilty of a public offense, punishable as follows:

...

(b) Any law enforcement agency that has knowledge of a violation of this section involving a constitutional officer of the state, a Member of the Legislature, or a member of the judiciary shall immediately report that information to the Department of the California Highway Patrol.

To implement this statute, the CHP established its Threat Assessment Unit and developed a proprietary threat database. The CHP threat database has been operational since 1987 and courts may submit requests for statistical data. The database can identify any cross- or multi-jurisdictional issues regarding threats and provide information specific to a suspect, the city of occurrence, the county of occurrence, or the specific member of the judiciary. Local law enforcement agencies may report threats to the CHP in any format they choose. When it is the law enforcement agency making the report, the CHP uses the Information Control Report, which has the primary data required for the database. A copy of the form is Attachment “G.”⁵³

Until recently, however, few sheriffs submitted reports to the CHP. From 1987 until July 2010, the CHP received approximately 255 reports of threats involving judges, an average of 11 reports per year. In 2010, the CHP met with the Court Security Committee of the California State Sheriffs’ Association to begin a partnership on outreach and education efforts regarding threat reporting, to create a safer state judiciary. This effort includes quarterly newsletters, the analysis of information reported, and guidance and assistance to local law enforcement investigators who are conducting these investigations. CHP has invited sheriffs’ deputies to attend the CHP’s Protection of Public Officials Course. CHP also provides two-hour and four-hour blocks of instruction for court security units and is developing a three-day Threat Assessment Investigations Course. CHP now maintains and regularly updates a complete list of contacts with all of the law enforcement agencies responsible for security in each of the 58 trial courts.

⁵³ Captain Jonathan Mobley of the CHP provided the information in this paragraph.

These efforts have increased compliance with reporting under Penal Code section 76. Over the last two years, CHP received reports of 174 threats, or approximately 87 reports per year. This represents a 791 percent increase in reporting.⁵⁴ However, California Penal Code section 76(b) only requires the reporting of threats to judicial officers.

The second statute requires state agencies to report to the CHP all crimes and criminally caused property damage on state-owned or state-leased property where state employees are discharging their duties. Government Code section 14613.7(a) provides:

- (a) Each state agency that is protected by the Department of the California Highway Patrol, those state agencies currently being protected by contract private security companies, or those state agencies currently under contract with a local governmental law enforcement agency for general law enforcement services, excluding all current mutual aid agreements, shall, as soon as practical, report to the Department of the California Highway Patrol *all crimes and criminally caused property damage* on state-owned or state-leased property where state employees are discharging their duties.

(Emphasis added.)

This statute is both broader and narrower than Penal Code section 76(b). Government Code section 14613.7 is broader in that it applies to *all crimes*; unlike Penal Code section 76(b), it includes threats and incidents involving individuals other than judicial officers, as well as criminally caused property damage. It is narrower in that it only applies to crimes that occur on “state-owned or state-leased property where state employees are discharging their duties.” Penal Code section 76(b) is not limited to these properties. There is also a difference as to which parties are responsible for reporting under the two statutes. Under Penal Code section 76(a), law enforcement agencies are responsible for reporting to the CHP; under Government Code section 14613.7, state agencies are responsible for reporting to the CHP.

1. The Appellate Courts

Currently, the Courts of Appeal and the Supreme Court report all crimes occurring in their facilities to the CHP because the CHP is responsible for providing their court security. These courts use the “STD. 99” form that CHP developed and which is Attachment “H” to this report.

The appellate courts are fortunate to have an integrated threat and incident program. The CHP receives reports on *all* threats and incidents related to these courts, whether they involve judicial officers, or other individuals, whether the crime involves persons or property, and wherever they occur within the state. The CHP’s Threat Assessment Unit then analyzes these reports and shares that analysis with the CHP units, or other local enforcement officers responsible for responding to the threat or incident. An integrated program is possible, because the appellate

⁵⁴ Captain Jonathan Mobley of the CHP provided the information in this paragraph.

courts use a single law enforcement agency with offices throughout the state. The appellate court members of the task force report that they are very satisfied with this program.

2. The Trial Courts

The trial courts face different circumstances. Local law enforcement agencies provide trial courts with court security. Although each sheriff and marshal may run an integrated threat and incident program within their respective counties, that program is not necessarily integrated with other counties, courts, or the state. Each sheriff and marshal is required to report threats to the CHP under Penal Code section 76(b), but the sheriff or marshal is the primary court security provider responsible for investigating such threats. Although the CHP is willing to assist sheriffs and marshals investigating threats to trial court judicial officers, staff, and immediate family members, CHP lacks the resources to investigate every threat in the state or to duplicate efforts of the sheriff or marshal charged with primary responsibility for investigating the crime. Moreover, trial courts are located in a variety of facilities, many of them owned by a county.

The law enforcement officials providing security for the trial courts are already under a statutory duty to report threats to persons associated with the courts to the CHP. Although these agencies have not always complied with this requirement in the past, the CHP has already undertaken and continues to make efforts to educate the sheriffs and marshals regarding reporting requirements. Moreover, the CHP has documented significant increases in compliance since undertaking its outreach and education efforts. Thus, the CHP is already responsible for collecting, analyzing, and disseminating information about threats and incidents involving both persons and property in the appellate courts and threats and incidents involving judicial officers in the trial courts. In addition, the CHP is already involved in educational and outreach efforts with the entire judicial branch and the law enforcement agencies that protect the courts.

Currently, however, incidents involving persons other than judicial officers or property used or occupied by the trial courts are not reported to the CHP. The sheriff and marshals providing security for the trial courts are not obligated to report to the CHP under Government Code section 14613.7, because the statute only requires compliance by “state agencies.” Moreover, Government Code section 14613.7 only applies to “state-owned or state-leased” properties. At least 200 of the 500 trial court facilities fall outside that description.

D. The Task Force Recommends that the Judicial Council Direct the Proposed Court Security Advisory Committee to Recommend a Branchwide Threat and Incident Reporting Program

The task force concludes that it is imperative that the branch have comprehensive and reliable statewide data on threats and incidents involving the courts. Such data is necessary to provide the best security for California’s judicial officers, court staff, and court users. Moreover, the branch needs the data to document the resources necessary for court security and to plan new courthouses.

The program should be coordinated with the CHP because it provides security to the appellate courts and the Supreme Court, and it has already implemented successful programs under Penal Code section 76 and Government Code section 14613.7(a). The program should also be coordinated with sheriffs' and marshals' offices because they provide security for the trial courts.

Therefore, the task force recommends that the Judicial Council direct the proposed Court Security Advisory Committee to:

1. Consider possible statewide programs, taking into account current law and practices outlined in this report and the necessity of coordinating with the CHP and sheriffs' and marshals' offices;
2. Make a recommendation to implement a program that provides for uniform reporting, assessment, and sharing of information regarding threats and incidents across the branch statewide and in coordination with the CHP and sheriffs' and marshals' offices; and
3. Make recommendations to seek changes in statute or rule of court to the extent necessary to implement the proposed program.

The task force strongly urges the Judicial Council to direct the proposed Court Security Advisory Committee to work on this proposal expeditiously because a branchwide threat and incident reporting program is needed immediately to assess and enhance the safety of judicial officers, judicial branch staff, and the public in California.

**Recommendation 4—
Continue to Review and Evaluate the Viability and Usefulness of Establishing
Branchwide Security Classification and Staffing Guidelines to Enhance the Safety
of California’s Courts.**

The task force recommends that the Judicial Council direct the proposed Court Security Advisory Committee to continue reviewing and evaluating the viability and usefulness of developing and establishing court security classification and staffing guidelines to Enhance the Safety of California’s Courts and make recommendations to the Judicial Council as appropriate.

Rationale for Recommendation

Personnel of many varied classifications currently provide security in courthouses throughout the State of California. These classifications include, for example, peace officers and corrections officers employed by the local sheriff, private security guards, retained by either the sheriff or the court, and marshals and court attendants who are employees of the court. The NCSC Report discusses the variety of classifications at greater length.⁵⁵ In addition to the variances in classifications, there are no standard guidelines on which classifications security providers should use for which security functions within the courthouse, and how many staff in each classification security providers should assign to each function.

This is the result of the historical development of court security. Prior to trial court funding, each county determined the funding and staffing for security in the superior courts. The enactment of the Superior Court Law Enforcement Act of 2002 reflected the change in the source of funding (i.e., from the county to the state), but did little more than maintain the status quo of funding levels for security in each trial court; the judicial branch never achieved the ambitious goal of raising all courts to a common level of law enforcement services.

The absence of statewide classification staffing guidelines has a number of consequences. It makes it difficult to compare trial courts and to determine a fair basis for allocating economic resources or achieving statewide efficiencies and cost-savings. The NCSC Report documents an apparent disparity between courts on security staffing, which may reflect inconsistent levels of security in courthouses throughout the state, but the lack of common standards makes this difficult to analyze and confirm.⁵⁶ In addition, the absence of statewide standards makes it more difficult and more expensive to estimate budget requirements and plan for new construction projects, courts, and facility upgrades. The absence of statewide standards means that each project must be based on an individualized assessment of the specific staffing context, rather than the use of a more global methodology.

⁵⁵ NCSC Report, pp. 2-2 through 2-6.

⁵⁶ *Id.* at p. 2-5.

The NCSC reviewed the current disparity in classifications and staffing levels in California trial courts and concluded that guidelines are needed to provide for the planning and allocation of California court security funding.⁵⁷ NCSC states that it is important for California to strive to put staffing guidelines into place, working with sheriff departments throughout the state.⁵⁸ Recognizing the fiscal and operational issues facing California, NCSC suggests that the Judicial Council work collaboratively with sheriff departments throughout the state “to establish a pathway toward a higher level of standardization in terms of both classification and staffing levels.”⁵⁹ The NCSC proposes, as an interim goal, a two-tiered system in which sheriffs’ deputies provide all courthouse security, with the exception of entrance screening stations, which courts would staff with unarmed guards under the guidance of at least one armed deputy.⁶⁰ The NCSC notes that this is consistent with the staffing and classification recommendations in its “Steps to Best Practices for Court Personnel,” which is an appendix to its report, and with the current practice in some California courts.⁶¹ The NCSC also concedes that migrating to a two-tiered system may result in additional costs.⁶²

Under court security realignment, the judicial branch is unable to enforce classification and staffing guidelines for sheriff’s staff because it no longer pays for those services. In addition, during discussions with the administration about the implementation of court security realignment, the administration made clear that it could not support legislation that would authorize or require court security classification and staffing standards or guidelines. The administration is concerned that imposing classification or staffing standards or guidelines would, to the extent they imposed new costs on the sheriffs, constitute an unfunded mandate under article XIII B, section 6 of the California Constitution.

Although the current fiscal and operational environments do not permit the development or implementation of guidelines at this time, circumstances change. The task force recommends that the charge to the proposed Court Security Advisory Committee include the responsibility to continue reviewing and evaluating the viability and usefulness of developing and implementing security classification and staffing guidelines, as the landscape of court security changes.

⁵⁷ *Id.* at p. 2-1.

⁵⁸ *Id.* at p. 2-12.

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

⁶¹ *Ibid.*

⁶² *Ibid.*

Recommendation 5—

Continue to Review and Evaluate the Court Security Plan Process to Facilitate and Increase Trial Court Compliance and to Ensure that Courts Establish and Keep Current All Necessary Procedures to Protect Every Person Entering a Courthouse.

The task force recommends that the Judicial Council charge the proposed Court Security Advisory Committee with responsibility for continuing to review and evaluate the process for preparing and submitting court security plans, and making recommendations to the council to facilitate and increase trial court compliance with Government Code section 69925. Preparation and maintenance of court security plans ensure that the court and sheriff or marshal establish and keep current all necessary protocols and procedures to best protect every person who enters a courthouse.

Rationale for Recommendation

Court security plans are critical tools for ensuring that the court and the sheriff or marshal address the physical security profile of a court and establish all necessary protocols and procedures to best protect every person who enters the courthouse. Requiring each court to develop a security plan ensures that the individuals responsible for court security consider and address in their practices and procedures all aspects of court security and to update and revise those practices and procedures as appropriate.

The NCSC in its report to the task force stated:

A court security plan establishes policies and procedures to be followed by security and court personnel in order to prevent and respond to court security incidents. The presence of a court security plan is integral to the safety of the courthouse; therefore, many states have adopted statutes and/or court rules requiring that all courts complete their own plan.⁶³

In California, Government Code section 69925 requires trial courts to prepare, in conjunction with the sheriff or marshal, a court security plan. California Rules of Court, rule 10.172 identifies the subject matter areas to be addressed in the court security plan. Rule 10.172 required trial courts initially to submit plans to the AOC on or before November 1, 2009. It requires trial courts to report any changes to the plan on or before February 1, 2011, and each succeeding February 1.⁶⁴ The AOC Office of Security is the AOC office that reviews the plans and any changes for completeness; it provides the court security plans and changes, together with a summary evaluation, to the Working Group on Court Security for its review.⁶⁵ The Working

⁶³ NCSC Report, p. 3-1.

⁶⁴ Cal. Rules of Court, rule 10.172(d).

⁶⁵ Cal. Rules of Court, rule 10.172(e).

Group on Court Security provides a summary of the court security plans and changes to the Judicial Council on or before July 1 of each year.⁶⁶ The council, in turn, submits to the Legislature each year a report summarizing all the reports and changes as required by Government Code section 69925.⁶⁷

AOC Office of Security developed an online interactive security plan template, which assists courts in preparing court security plans. In addition, AOC Office of Security staff will, at the request of a court, make themselves available to assist courts individually.

Initial compliance with the requirements to prepare and submit court security plans was disappointing. As of March 2010, only 14 of 58 trial courts had submitted security plans representing a 24 percent compliance rate. After AOC Office of Security staff followed up with the trial courts in April 2010, the compliance rate increased to 41 percent, with 24 of 58 courts submitting plans. By August 7, 2010, the Judicial Council was able to report to the Legislature that 39 of the 58 trial courts (67 percent) had submitted plans, but of these, only 30 plans were considered complete.⁶⁸

When the task force met in June 2010, it identified improvement in compliance rates as an area on which the NCSC could advise the task force. The task force and the NCSC eventually agreed that one section of the NCSC's report would address methods for improving trial court participation and the timely submission of court security plans in compliance with Government Code section 69925.

While the NCSC worked on the report, the task force made its own effort to increase compliance. Working with AOC Office of Security staff, members of the task force contacted individual courts to encourage submission of complete reports. This effort was successful. By July 2011, the Judicial Council reported to the Legislature that 49 of 58 trial courts (84 percent) had submitted plans, all of which were complete or in the process of being revised for completeness so as to be in compliance with Government Code section 69925 and California Rules of Court, rule 10.172.⁶⁹

In its final report, NCSC devoted one section to court security plans.⁷⁰ In that section, the NCSC provided the task force with information on court security plans in five other states, reviewed the subject matter areas identified in California Rules of Court, rule 10.172, and made several recommendations. Given recent improvement in compliance, the task force concluded that the NCSC's recommendations are not necessary.

⁶⁶ *Ibid.*

⁶⁷ Former Gov. Code, § 69925(a). The Legislature repealed this requirement, effective June 27, 2012. (SB 1021; Stats. 2012, ch. 41, § 33.)

⁶⁸ Judicial Council of Cal., Annual Report Summarizing Court Security Plans, dated Aug. 27, 2010, p. 3.

⁶⁹ Judicial Council of Cal., Annual Report Summarizing Court Security Plans, dated July 1, 2011, p. 3.

⁷⁰ NCSC Report, pp. 3-1 through 3-15.

California Rules of Court, rule 10.172 currently requires submission of court security plans to the Working Group on Court Security. The administration, in late May 2012, proposed budget trailer bill language that would, if enacted, repeal the statutory authority for the Working Group on Court Security. If that group is disbanded, then it would be appropriate to make the proposed Court Security Advisory Committee responsible for the review of court security plan submissions and reporting on that review to the Judicial Council. In addition, court security is a dynamic area. The task force recommends that the council charge the proposed Court Security Advisory Committee with a continuing responsibility for considering any changes to the rules of court governing court security plans and recommending to the council any changes necessary to facilitate and increase trial court compliance with Government Code section 69925 to improve the administration of justice.

**Recommendation 6—
Further Develop Court Emergency Planning Tools and Increase Associated
Educational Efforts about the Tools to Provide Safe and Accessible Courthouses.**

The task force recommends that the Judicial Council direct the AOC Office of Security to (1) disseminate information to educate judges and judicial branch staff about the emergency planning tools, programs and assistance that it makes available to the courts; (2) further develop the emergency planning tools; and (3) allocate to the AOC the resources to implement this direction because emergency planning is necessary to provide safe and accessible courthouses.

Rationale for Recommendation

In 2006, the Conference of State Court Administrators (COSCA) recognized the importance of emergency planning for maintaining the rule of law during a crisis:

Recent disasters have demonstrated that an immediate mobilization of the justice system—including the country’s state court systems—is essential to support societal stability and protect individuals, families, businesses, and institutions. . . . [¶] . . . an operational court system capable of performing constitutionally mandated functions stands against the chaos created by an emergency and ensures that the judiciary can fulfill its mission of maintaining the rule of law, protecting individual rights, and providing for the prompt and lawful processing of those charged with crimes.⁷¹

The AOC Office of Security takes the lead in emergency planning activities for the judicial branch. Indeed, when it was first established in 2005, the AOC Office of Security’s original charge was to facilitate development of emergency planning tools for the trial court and AOC facilities. By 2006, the AOC Office of Security had reviewed most of the systems used by individual courts or promoted by national organizations, including the NCSC, Federal Emergency Management Agency (FEMA), and the California Emergency Management Agency (Cal EMA). The AOC Office of Security determined that the ideal system had to be easy to maintain and operable by persons without previous experience in emergency planning and with a minimum amount of specialized training. Due to the number and complexity of the court facilities across the state, AOC Office of Security determined that a web-based program would be the most suitable for the judicial branch.

The AOC began, in 2007, by purchasing from Bold Planning Solutions a Continuity of Operations Planning System tool with a demonstrated record of success at other public sector entities. FEMA defines a Continuity of Operations Plan (COOP) as an internal effort within

⁷¹ COSCA, Resolution I, Emergency Preparedness in the State Courts (Dec. 2006), <http://cosca.ncsc.dni.us/Resolutions/resolutionEmergencyPreparedness.html>.

individual components of a government to ensure the capability exists to continue essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. This means that each functional unit within the court organization must be prepared to continue providing basic services to constituents and preserving essential facilities, equipment, and records. Each unit must be ready during a wide range of disruptions, from a broken water line in a single facility to a devastating earthquake affecting an entire region.

The AOC made the initial purchase of the COOP tool with funds from a grant from the United States Department of Homeland Security. It is simple to use, working much like web-based, user-friendly tax preparation software that guides court staff through a series of questions, resulting in the generation of a completed plan. The resulting plan meets the COOP planning requirements of the government sector mandated for the federal government by Presidential Decision Directive 67 (PDD 67) and FEMA Federal Preparedness Circular 65 (FPC 65). The courts' plan, including all necessary information, is securely preserved and accessible on fully redundant sites located out of state. The AOC Office of Security offers training and access to the tool at no cost to all courts; the training and completion of the COOP does require valuable court staff time.

The AOC Office of Security continues to develop and enhance the web-based emergency planning tools that it makes available to the courts. In 2009, the AOC Office of Security made available to the courts an Emergency Response Plan tool, similar to the COOP tool and purchased from the same vendor. In contrast to COOPs, which are designed to facilitate a court continuing all essential functions within 12 hours of an emergency and sustaining those functions for up to 30 days, an Emergency Response Plan is intended to address the court's response in the first 72 hours following an emergency. Beginning in the summer of 2012, the AOC Office of Security will make available to the courts a Command and Control Plan tool, which addresses court executive team functions in managing the overall incident for courts with a large employee count or multiple facility locations.

The AOC Office of Security's COOP program has attracted attention from courts throughout the world. AOC Office of Security staff have been invited to give presentations about COOP planning at conferences and meetings around the country. In 2011, representatives of the Supreme Court of Japan visited the San Francisco AOC headquarters for in-depth briefings about the COOP program.

By mid-2012, the AOC Office of Security had trained 92 percent of the California trial courts on using the COOP tool and had begun work on their COOPs. Only 26 percent of courts have complete and current plans, although many are close to being final and are completely usable at this time. In 2011, the AOC Office of Security held training sessions in Los Angeles and San Francisco for the appellate courts and achieved 60 percent participation. The AOC Office of Security has not begun tracking court use of the Emergency Response Plan tool.

Court staff have informed the AOC Office of Security that, given competing demands, they lack time to attend trainings or to complete the COOPs; some believe that additional help from AOC Office of Security staff would assist in completing COOPs. In addition, court staff report that many in the judicial branch are unaware of the availability of the planning tools, the actions they are expected to take in the event of an emergency, or the importance of planning in advance for such events.

The task force finds that the emergency planning program offered by the AOC Office of Security is important for assuring the continuation of court services following a disaster.⁷² For the program to be completely effective, however, more courts must participate and complete the available emergency planning tools. To that end, the task force recommends that the Judicial Council direct the AOC Office of Security to (1) disseminate information to educate judges and judicial branch staff about the emergency planning tools, programs and assistance that it makes available to the courts; (2) further develop the emergency planning tools; and (3) allocate to the AOC the resources to implement this direction because emergency planning is necessary to provide safe and accessible courthouses. In particular, the task force recommends that information about the availability and importance of emergency planning tools be incorporated into educational venues such as the B. E. Witkin Judicial College of California and the New Judges Orientation.

⁷² Although the SEC report recommended against the AOC Office of Security performing a number of functions, it apparently concurs that the office should be involved in emergency planning. Recommendation 7-55 of the SEC Report includes “review of emergency plans,” as an example of a program upon which the office should focus. (SEC Report, p. 147.)



California State Court Security Report

Threat and Incident Reporting

**Court Security Personnel Classification
and Staffing Level Standards**

Court Security Plans

Final Report – March 2012

Timothy F. Fautsko, Project Director
Steven Berson, Project Consultant
Steve Swensen, Project Consultant
Nathan Hall, Project Staff
William Rafferty, Project Staff

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

Executive Summary

The mission of the National Center for State Courts (NCSC) is to improve the administration of justice through leadership and service to state courts, as well as to courts around the world. Through its research, consulting services, publications, and national educational programs divisions, the NCSC offers solutions that enhance court security, emergency preparedness, disaster recovery and continuity of operations based on the latest guidelines and information on best practices guidelines. The NCSC's Court Consulting Services Division located in Denver has extensive experience in conducting local and statewide security assessments. The NCSC also assists the Conference of Chief Justices, the Conference of State Court Administrators, as well as state and local courts across the nation.

The NCSC was engaged by the Office of Emergency Response and Security (OERS) within the California Administrative Office of the Courts (AOC) as the staff entity to the California Judicial Council, Court Emergency Response and Security Task Force, to address the following three topics: Threat and Incident Reporting; Analysis of Court Security Classification and Staffing Level Standards; and Court Security Plan Review. For each of these topics the OERS asked the NCSC to research what other court jurisdictions are doing nationally and to make recommendations for improvements in California. The following presents an executive summary for each topic listed above. It should be noted that substantial changes have recently occurred in California with regard to court security funding. In 2011, the Governor's Office together with the California Department of Finance transferred court security funding from the judicial branch directly to the counties for reimbursement of the Sheriffs. This essentially has limited the oversight capability of the courts over their security providers.

Threat and Incident Reporting

In order to respond effectively to threats and to manage incidents in an appropriate fashion, it is imperative that courts have a solid, structured reporting process in operation. A standardized mechanism for reporting threats and incidents is an extremely important aspect of a court's security program. The NCSC surveyed the following six jurisdictions to gather information on their threat and incident reporting systems: New Jersey; Pennsylvania; Texas; Utah; Washington; and Federal Courts/United States Marshal Service (USMS). For each of

these jurisdictions, the NCSC gathered information on reporting requirements, general data included in the reports, and the processes involved in reporting. This report recommends the following components for a solid threat and incident reporting system: a standardized, user-friendly reporting form; a functioning definition of what is a threat or an incident; and a clear assignment of responsibility for reporting and recording threats and incidents. The report also discusses the elements and advantages of an electronic reporting system.

Court Security Classification and Staffing Level Standards

Security is currently provided in courthouses throughout the state of California by personnel of various classifications. These classifications include, for example, sworn peace officers, corrections officers, contract guards, and court attendants. In addition to the variances in classifications, there is little in the way of staffing standards in terms of how many officers should be assigned to various security functions within a courthouse. This makes it increasingly difficult for OERS to assist in designing optimal security staffing, to evaluate planning proposals, and to estimate personnel and budget requirements on new court construction projects and facility upgrades. Minimum standards are needed to provide for the planning and allocation of California court security funding. The NCSC confidentially surveyed nine jurisdictions to gather information on classification and staffing levels for security personnel. In addition to gathering information from the sample jurisdictions, the NCSC analyzed its own best practices guidelines for courthouse security in an effort to determine what might work best for California. These guidelines have been developed over the past several years as the NCSC has conducted security assessments of over 230 courthouses throughout the country.

Based on the information gathered in the sample jurisdictions and on the NCSC best practices guidelines, the report makes recommendations for California to move toward more standardization regarding classification and staffing levels for security personnel. A reasonable and achievable goal is that the basic classification of sheriff deputy could serve in all functional areas of courthouse security, with the exception of screening stations. Unarmed guards could staff entry screening stations with at least one armed deputy assigned to oversee each station. The NCSC best practices guidelines can serve as a useful framework for the California courts to address staffing standards. The Judicial Council could adopt the NCSC best practices guidelines as aspirational goals and take steps to achieve it. The NCSC's steps approach to best practices

with respect to staffing levels is an appendix to the report and provides a realistic a means of achieving that goal over time.

Court Security Plans

A court security plan establishes policies and procedures to be followed by security and court personnel in order to prevent and respond to court security incidents. California adopted a rule requiring state courts in the 58 counties to develop court security plans, but the state struggled with compliance on its first year of the new rule among its trial courts. California has also created an online security plan template to assist courts in generating security plans. For its report, the NCSC reviewed statutory and court rule requirements, as well as administrative policies, techniques and governance structures relating to security plans in the following five states: Arkansas, New Jersey, Ohio, Oregon and Utah. Based on information gathered from these states, the report recommends approaches for California to improve compliance with its security plans requirement. These approaches include: continuing to promote the use of the California online security plan template and completion tool; enhancing and augmenting the online model security plan content to provide local courts more resources when completing online security plans; increasing AOC Security Coordinator manpower to assist in local court security plan development; creating a security improvement grant fund; and initiating stricter enforcement of existing court orders.

Summation

A detailed analysis of each topic listed above is contained in this report. However, it is important to note that analysis without subsequent action is often futile. OERS has an opportunity to present NCSC's analysis of the three topics to members of the California's Judicial Council's Court Emergency Response and Security Task Force. Implementation of the many recommendations contained in the NCSC report will serve to improve court security and to better protect the public as well as judges and court staff in the state of California.



California State Court Security Report

Threat and Incident Reporting

Final Report – March 2012

Table of Contents

I.	Introduction	1-1
II.	Importance of Threat and Incident Reporting.....	1-1
III.	Threat and Incident Reporting Currently in Place in California.....	1-2
IV.	NCSC Survey.....	1-3
	A. Reporting Requirements in Surveyed Jurisdictions	1-4
	B. Data included in threat and incident reports in surveyed jurisdictions	1-4
	C. Process for Reporting.....	1-7
V.	Recommendations.....	1-7
	A. The Reporting Form.....	1-9
	B. Responsibility for Reporting.....	1-10
	C. Electronic reporting systems	1-11
	D. Managing the system.....	1-13
VI.	Conclusion	1-14
	Appendices.....	A-1-15

I. Introduction

The National Center for State Courts (NCSC) was engaged by the Office of Emergency Response and Security (OERS) within the California Administrative Office of the Courts (AOC), as the staff entity to the California Judicial Council, Court Emergency Response and Security Task Force, to address the topic of threat and incident reporting. Specifically, the OERS requested that the NCSC complete the following tasks:

- A. Evaluate statewide threat and incident reporting systems that may be utilized by other states or agencies to determine the basic information requirements, process for reporting threats and incidents and process for dissemination of the data to other agencies.
- B. Evaluate the findings from the Task Force and compare the best process with those reviewed from other agencies.
- C. Make recommendations for California based on the most effective process, most likely format required by future federal systems and the most cost effective approach.

II. Importance of Threat and Incident Reporting

We live in a time when threats and acts of violence are directed toward judges as a result of their official duties. It is crucial that every threat directed against a judge be taken seriously and assessed. We also live in a time when incidents frequently occur within a courthouse. Incidents can include matters ranging anywhere from someone trying to bring a weapon into the courthouse, to someone being abusive to a court clerk at a public counter.

The number of threats and violent incidents targeting the judiciary has increased dramatically in recent years. At the federal level, the U.S. Marshals Service reports the number of opened judicial threat investigations has almost tripled from FY 2002 (565-cases) to FY 2010 (1,580-cases). At the state level and local level, the most informative data comes from studies conducted by the Center for Judicial and Executive Security (CJES). In one such major study, Judicial Counter-Violence Initiative /Court-Targeted Acts of Violence (JCVI/CTAV), CJES has documented 148-incidents of state/local courthouse shootings, bombings, and arson attacks from 1970-2009. These 148 incidents included 13 assassinations and 18 assaults against state or local judges. There was a total of 254 victims in these 148 incidents, with 147 persons killed and 107 seriously wounded. The CJES study documented a decade-by-decade escalation in courthouse

violence, and it contains conclusive research findings on threat source intent, motive, targets, and victims. As part of its efforts to update its JCVI/CTAV study, CJES has to date documented 40 additional incidents of courthouse violence.

CJES has also published *Incidents of Disorder in the Court* which documents other acts of courthouse violence (e.g., knifings, murder plots, assaults, suicides, etc.) not delineated under CTAV Study criteria. The *Incidents* publication, listing security incidents from January 2005 through May 2011, is updated bi-monthly. Currently, CJES has documented a total of 135 court security incidents under this publication. The number, extent, and type of these incidents (in addition to the incidents included in the JCVI/CTAV study) provide a compelling justification for the need for good court security.

To be able to respond effectively to threats and to manage incidents in an appropriate fashion, it is imperative that courts have a solid, structured process in place. A standardized mechanism for reporting threats and incidents is an extremely important aspect of a court's security program. A good system will not only allow courts to respond more effectively to each threat or security incident, it will also allow courts to analyze threats and incidents in the aggregate, providing guidance for making improvements to overall security within the courthouse.

III. Threat and Incident Reporting Currently in Place in California

According to the OERS, the California penal code requires that all threats against judges be reported to the California Highway Patrol (CHP). Historically, relatively few threats are reported. However, the CHP has recently engaged in an educational effort with local law enforcement to help them understand the criticality of reporting these events in a timely fashion. This effort, together with the internal data retention by CHP, has improved the program. There is no statutory requirement for the reporting of other crimes or incidents in courthouses to any agency outside of the law enforcement entity who has taken the event report. There is no statewide reporting/gathering process in place. There is no clear process in place to specify how threats and incidents should be reported and no clear path of communication among the many agencies and jurisdictions involved. Because of the lack of a process and a system for reporting, managing, or tracking incidents, there is little meaningful data that can be used to substantiate

need and request related funding and services. There is no system to share threat data among California agencies, and with counterparts on the federal level, and no central database that can be accessed by the administrative office, courts and security providers.

In 2007 the OERS conducted a first-ever statewide survey of judges and justices concerning threats they had received. The survey reached over 1600 judges and justices, and there was a response rate of 53%, representing 92% of courts in the state. A total of 296 threats were reported in the survey. Of these:

- 75% of the total was against a specific judge, employee, or family member.
- 72 threats were described as imminent.
- With respect to threats that were classified as general rather than imminent, when the threat was related to a case, the cases were predominately criminal or family. Over half the time, the plaintiff or defendant in the case was the person who made the threat.
- 83% of the total threats were reported, most often to the sheriff.
- 85% of the judges and justices said that the threat had been investigated to their satisfaction.
- 79% of the judges and justices said that they received feedback on the investigations.
- Many judges reported being threatened at their residences, where they are often without protection.
- Many judges and justices said they were threatened right outside of the courthouse.
- 94% of the judges and justices said they feel safe in their home; 92% said they feel safe on the bench; 87% said they feel safe in the courthouse.

IV. NCSC Survey

To address the tasks assigned by the OERS, the NCSC surveyed the following sample of six jurisdictions to gather information on their threat and incident reporting systems:

- New Jersey
- Pennsylvania
- Texas
- Utah
- Washington
- Federal Courts/United States Marshal Service (USMS)

The states of New Jersey, Pennsylvania, and Texas were selected as part of the sample in

order to match closely with the physical size and large population of California. The states of Utah and Washington were included due to their proximity to California. Finally, the federal courts were included due to the extensive work and expertise of the USMS in the areas of incident reporting and threat management.

A. Reporting Requirements in Surveyed Jurisdictions

Most states surveyed have rules of court or administrative policies requiring the chief judge and/or court administrator to report court security incidents or threats. Pennsylvania Rule of Judicial Administration 1954 places the burden of reporting squarely within the judicial branch. The chief judge in each district is responsible for ensuring that the district court administrator enters the necessary data into Pennsylvania's judicial system incident reporting system the same day that the incident occurred. New Jersey has developed policy directives through its Administrative Office of the Courts that have the effect of requiring all security incidents be reported to a court director or administrator (see for example, http://www.judiciary.state.nj.us/directive/municipal/dir_15_06.pdf). The state of Washington through its Board of Judicial Administration's Court Security Committee, established court security standards that include the reporting of incidents to the AOC. <http://www.courts.wa.gov/newsinfo/content/pdf/securitystandards.pdf>.

Court rules or policies are not binding upon the other branches or levels (e.g., local) of government. State statutes are generally binding, but are rare with respect to incident reporting. Texas is perhaps one of the only states with a statute directly on point (Code Crim. Proc. art. 102.017): To wit, "A local administrative judge shall provide to the Office of Court Administration of the Texas Judicial System a written report regarding any security incident involving court security that occurs in or around a building housing a court for which the judge serves as local administrative judge not later than the third business day after the date the incident occurred." Utah's laws (Utah Code Ann. § 17-22-27) require "The state court administrator can enter into a contract with the county sheriff for bailiffs and building security officers for the district and juvenile courts within the county." Note: The state court administrator in Utah is a comparable position to the administrative director of the courts in California.) It is this contract that requires reporting to the state court administrator's office. In addition, California has a law requiring that any threat against a member of the judiciary must be

reported to the California Highway Patrol. Penal Code, Section 76 (b).

B. Data Included in Threat and Incident Reports in Surveyed Jurisdictions

The jurisdictions surveyed yielded a variety of specific threat and incident reporting forms. These forms are attached to this report as Appendices A through F. This section describes more generally the data elements included in the forms.

The states surveyed vary in terms of the definition of an “incident.” Two states include the definition of an incident in the reporting form itself. The New Jersey form specifies that an incident report be filled out “when you witness, are involved in, or are informed of a security incident such as a threat, assault, display or use of a weapon, escape from custody, theft, disorderly conduct, or disruptive behavior.” The Washington State form states that an “incident means a threat to or assault against the court or court community, including attorneys, court personnel, jurors, litigants, witnesses of others using the courthouse. It also includes any event or threatening situation that disrupts the court or compromises the safety of the court or the court community.”

At the federal level, the Court Security Improvement Act of 2007 outlined the use of grants for states to develop threat assessment databases. Unfortunately, to date those funds have never been obligated. Consequently, it does not appear that the development and implementation of a national threat management database or incident reporting system is imminent. States developing incident reporting systems should proceed with the understanding that at present time there are no recognized national guidelines. In all likelihood it will be the “up-and-running” state systems that will be looked upon as possible models for developing national systems and guidelines.

All state courts and the federal system surveyed require that the reporting form include the name of the court and its address. Four of the five states also identify court type either on the form or (in the case of Texas) by the use of separate forms for separate court types. Required contact information also varies. New Jersey asks for a phone number, while Texas and Washington State obtain both phone and email information. All states and the federal court surveyed require that the date and time of the incident be reported. Case types are required in Utah, while Texas and Pennsylvania require case type and case numbers/captions.

New Jersey, Pennsylvania, Texas, and Utah all provide spaces to indicate whether the individual(s) involved is a criminal defendant, juvenile respondent, civil plaintiff or defendant, or member of the general public. Texas and Utah further specify if the individual(s) involved is a family member or friend of a party to the case. In terms of the type of incident, four states and the federal courts provide for an indication of a physical assault. Utah includes a separate category of “fight” and the federal courts have a “shooting” option separate from assault. New Jersey, Pennsylvania and the federal courts include disorderly or disruptive behavior as well. Additionally, Texas includes hostage taking as an option. New Jersey, Utah, Pennsylvania and the federal courts specify damage, vandalism and theft as options. The federal courts further differentiate vehicle break-ins and burglaries. Other options are arson (Utah and Pennsylvania) and forced entry or trespass (federal, Utah).

All states surveyed attempted to determine whether a threat was transmitted by mail, phone, in person, or through other means. This last category is subdivided into email (Pennsylvania, Utah, Texas, Washington) and through a third party (Utah). Both Pennsylvania and Utah treat verbal or personal threats as both a threat *type* and a threat *mode*. Four states plus the federal courts identify bomb threats and threats posed by suspicious packages.

Pennsylvania has by far the most expansive listing of possible emergencies, including fire, medical, escape, contamination, and weather. Utah includes the same list but excludes weather. New Jersey tracks fires and escapes. Federal courts track medical injuries only and Texas tracks only attempted escapes. Other incidents include attempt to bring drugs (Pennsylvania, Utah), weapons (federal, Texas) and “contraband” (federal, Utah).

The reporting forms of three states (New Jersey, Pennsylvania, Texas) require information as to where within or around a court an incident takes place, with specific locations including courtroom number, chambers name or number, staff office name or number, parking lot or garage, and holding cell. Additionally, New Jersey and Pennsylvania identify whether the incident occurred at a specific entrance.

New Jersey, Pennsylvania, Texas, and Utah all ask whether a weapon was used in an incident, although only Pennsylvania and Texas ask for a specific type (e.g., knife vs. firearm).

Pennsylvania, Texas, Utah, and Washington specifically ask if the incident resulted in injuries and whether medical attention was required.

New Jersey and Pennsylvania asked who was involved in the incident – including those individuals targeted by the threat(s). Texas asked who the incident perpetrator was (but not others involved) and also who the threat was made against. All requested specific information on what officials and persons (e.g., judges, court staff/employees, law enforcement officers, attorneys, jurors, witnesses, litigants, prisoners, and others) were involved in the incident.

Because not all incidents are crimes, not all incident reports will indicate law enforcement involvement. Federal courthouse security is provided by USMS; therefore all incident reports in the federal system involve law enforcement. However, the states do ask if law enforcement was involved in the incident, and, in the case of New Jersey and Texas, specifically if an arrest was made.

C. Process for Reporting

All states and the federal courts recognize the possibility that an incident report will be filled out by law enforcement. However, as noted above, the responsibility for initially reporting in the state courts rests with non-law enforcement court personnel or judges. Moreover, in Texas it is expressly the administrative judge who transmits the incident report to the AOC. Three states and the federal courts provide for online or electronic transmission of the forms. Utah has a similar system in place but at this writing has not implemented it due to lack of funding and, along with Texas and Washington, continues to rely on some paper mode (fax, mail, email attachment). All states transmit their incident reports to their respective AOCs, either to a particular named person or department. Since the federal courts are protected by an arm of the executive branch, the information is transmitted to the USMS.

V. Recommendations

A good reporting system will notify the appropriate officials of threats and incidents in a timely manner, and will provide essential information to allow the problem to be properly assessed, investigated, and handled. Court staff may observe something that appears problematic

(e.g., a door to a secure area is propped open). Without an incident reporting system in place, this problem may go unreported and uncorrected. More serious and obvious incidents, such as someone pulling a gun outside a courtroom, will be dealt with even if there is no incident reporting system in place. An incident reporting system will provide the information to respond to all incidents properly, whether obvious or subtle. It will provide information to enable authorities to investigate, apprehend, and convict perpetrators.

An optimal incident reporting system will advise the appropriate (i.e., designated) officials of court security incidents in a quick and timely manner, and provide the essential information for the situation to be properly investigated, analyzed, assessed, and action taken. Policies and procedures should be established on both local and state levels to instruct judicial officers, staff, and others on who the designated appropriate officials are for initially receiving and processing incident reports. Designation is dependent on primary jurisdiction and other-related factors (e.g., state statutes, guidelines, court security committee resolutions, resources, law enforcement presence, etc.). However the responsible authority or central receiving component (i.e., designated officials) should be situated within the courts and law enforcement organizations.

It is also essential that designated officials maintain a certain level of knowledge and familiarity on the basic principles of judicial threat management. Due consideration should be given to reporting, investigating, and assessing “inappropriate-communications” (to include suspicious behaviors and activities) which are potential pre-indicators of violent behaviors/actions, but by themselves are not incidents. With adequate training and understanding this can and should be accomplished at a local level.

In general an incident reporting system provides the information required to accomplish the following objectives: properly document, assess, and manage incident specifics and variables; conduct a comparative analysis between past incidents and outcomes; increase overall court security awareness; and coordinate with the appropriate authorities on case investigations – to include apprehension and prosecution efforts. These objectives pertain whether incident reporting is conducted at the state level or remains, relative to the incident type and extent, solely a local concern.

While incident and threat definitions are presented below, it is important to understand the difference between the two. A threat is always considered an incident – but an incident is not always a threat. Threats are likely violations of law, while certain incidents may not be. Incidents may in fact be “inappropriate-communications” or relatively lesser-degree incidents such as equipment malfunctions, violations of established security protocol, courtroom disturbances, and the like. Certain incidents may be important enough to document and respond to at a local level, but are not necessarily the type or extent of incident requiring reporting to the state. To ensure however that the appropriate numbers of incidents are in fact being reported to the state, it is necessary to clearly delineate the reporting requirements. On a local level “Suspicious Activity Reports” (SAR) and a “Security Management Activity Report Tracker” (SMART) system can reasonably, efficiently, and cost-effectively handle “lesser” type incidents.

A. The Reporting Form

A good threat and incident-reporting system begins with a good standardized form. The standardized threat and incident reporting form should be user-friendly to assist the preparer in promptly providing essential information with relatively little effort. A check box or checklist format can substantially simplify the process. The tendency to collect too much information about a threat or incident will often reduce "user friendliness" and will create reluctance to use the form, which can result in the collection of only minimal information.

A functioning definition of what is a threat or an incident is required and definitely should be included as a portion of the threat or incident report. Not every activity involving the presence or actions of law enforcement is an “incident.” Nor is every incident a crime (although, without question all crimes are incidents). The definition, therefore, should contain a restrictive list of broad categories (Actions against Persons, Actions against Property, Threats, and Emergencies) with subcategories that provide additional detail.

A limited number of federal agencies have defined incidents and threats based on their individual jurisdictions and mission duties and responsibilities. However, none has defined “incidents” from a court-operations perspective. Only the USMS has defined “threats” as it primarily relates to court security. Recommended language for defining a *court-specific incident*

would include the following: “an event, natural or man-made, that requires a specific emergency and/or law enforcement response in order to protect and preserve life or property.” Recommended language for defining a *court-specific threat* would include the following: “explicit or implied communications, whether written, verbal, third-party, or behavior-based; of intent to assault, impede, intimidate, or interfere with the judiciary, including a judges family and court employees.”

The minimal components of a threat or incident report are reporter information, including a phone number for follow-up, court name and address, location within or in proximity to the courthouse, and time and date information. Identification of case types can provide broader strategic information that may indicate whether certain case types are more prone to spark incidents. However, the particular case and the status of the individuals involved (parties, family, etc.) would be more useful for operational control of potentially volatile situations. Therefore, both should be included.

B. Responsibility for Reporting

The responsibility for reporting threats and incidents should reside in the judiciary and executive branches (through the sheriffs). The responsibility for recording them should reside in the judiciary. At the local level, the Pennsylvania model seems the most flexible as overall responsibility is placed on the president (i.e., chief) judge of a district (most districts consist of a single county) court while the chief court administrator (the equivalent of a court executive officer in California) is responsible for day-to-day data entry.

In the alternative, or for those counties or courts that have few incidents, this may result in the chief judge submitting the information (similar to the Texas model). Regardless of the person responsible for entry of the incident, the report should be transmitted to the Administrative Office of the Courts. In California it is envisioned that these reports would also be simultaneously forwarded through the respective regional (i.e., Northern/Central Region, Bay Area/Northern Coastal Region, and Southern Region) offices of the Administrative Office of Courts. This process will ensure that all incidents are properly documented and followed-up on.

There seems to be two schools of thought about verification and review of threat or incident information. One approach is to have an eyewitness to an event promptly and

independently fill out an incident report form and transmit it to a designated court administrator or law enforcement agent for inclusion in an existing paper-based repository or electronic database. In such circumstances, the form will be referred to the proper security official for follow-up, but there will be no official approval or editing of the form. This approach is based on the belief that it is better to capture more information quickly and directly from the person who witnessed the security event. On the other hand, there are those who believe a security-incident form should be subject to oversight or approval before the information is officially transmitted for inclusion in the database and/or forwarded to a responsible official for follow-up. Upon receipt, the supervisor would review the document as soon as possible and, where necessary, follow up with the sender to offer assistance and ascertain that the information provided is understood and that no significant details have been omitted. This approach is based on the belief that it is better to restrict incident-reporting to those persons who have received appropriate training regarding what incidents and related information should be entered into the database. Proponents also contend that this approach promotes greater accuracy and consistency.

It is recommended that a variation of the latter approach be used for incident reporting. To allow for incident facts to be ascertained, incident reports should be submitted to the designated official no later than two or three days from the date of the incident. That does not mean prompt notice of the incident cannot be conducted prior to report submittals. For all practical intents and purposes, communications should also be established where designated officials are made aware of incidents as they transpire with the understanding an incident report will follow. A trained court security or law enforcement officer should always be involved (i.e., the reviewing/approving official) in any incident requiring reporting. This will not only ensure complete and proper documentation, but also provide a single point-of-contact to facilitate incident follow-up.

C. Electronic Reporting Systems

Ideally, the threat and incident report should be recorded and transmitted electronically. This is by far the optimal means for such communication, linkage to other information sources (such as law enforcement, case management systems, etc.), and timeliness. Timely transmission of the reports is important. There should be a specified time from the occurrence and reporting of the incident to the completion and submission of an incident report. Recipients of the reports

should be clearly identified. Appropriate recipients may include court administration (state and local), the local or state security committee, facility management, and law enforcement. The successful management of threats against judicial officers requires a state judiciary to have a solid information system that serves the following essential purposes:

1. Allow the appropriate court official to effectively collect and input data concerning actual or potential threats made against a judicial officer in his local court; this includes communications or actions that are clearly threats as well as inappropriate communications and contacts that need to be reported and assessed for threat signatures.
2. Allow every court official access to data about threats and perpetrators from other locations throughout the state and beyond.
3. Provide a secure data base for those responsible for threat management to evaluate threats and to track appropriate responses.
4. Equip the courts with the capability to conduct assessments and facilitate a coordinated threat mitigation process with the law enforcement and other criminal justice stakeholders.

There should be a repository of information relating to potential threats and the information in that repository must be shared with appropriate persons. When a court receives a threat against a judge, a determination needs to be made by the designated court official and by local law enforcement as to the seriousness of the threat and the appropriate response. It is imperative that no threat be ignored. There should be rigorous protocols in place that require recording, evaluation, and follow-up with respect to all threats. Some threats may require little or no response, while others may require a significant level of action to protect a judicial officer. Subsequently, a system needs to be in place to track threats to insure that the appropriate officials are aware of each threat and that appropriate action is taken. A threat cannot be properly evaluated without full and ready access to all relevant data about the person or persons making the threat. Questions should be asked. Does the person have a criminal record? Has he or she made other threats or acted improperly elsewhere? This important information may reside outside the jurisdiction of the local court and outside the state. It may reside with one or more local, state or federal law enforcement agency.

The Pennsylvania Judicial Security Incident Reporting System (PAJIRS) was the first court-initiated electronic incident reporting system in the country. Implemented in August 2007 PAJIRS is a password sensitive automated software program for reporting incidents under the

state courts Unified Judicial System of Pennsylvania. There are a number of commercially available incident reporting software programs. However most if not all of these were developed to address incidents from a wide-range threat management perspective, and law enforcement investigative position, and would need considerable re-programming to effectively address court-specific incidents. The primary emphasis for private software companies has been workplace and school violence programs. The United States Marshals Service (USMS) utilizes its Justice Detainee Information System (JDIS-8 version) to document, investigate, assess, and manage inappropriate communications (i.e., incidents) made against judicial protectees and court facilities. JDIS-8 is not a “stand-alone” system in that it also is the primary database for USMS warrants, criminal investigations, and prisoner processing, tracking, and scheduling. The USMS also documents “incidents” at screening stations and security patrols/posts through its Court Security Officer (CSO) monthly statistical summary – a standardized form. At this writing, there are no plans by the USMS to develop a specific software program for incident reporting and judicial protective intelligence and investigations programs.

The automated approach provides for greater speed in reporting and responding to threats or incidents, and it facilitates creation of an easily searchable database of bulk information. In addition, such database information can also be easily and quickly shared among authorized users. A court should not wait until an electronic system is established before installing some level of incident reporting. It is more important to begin with a manual, hard-copy system rather than wait.

D. Managing the System

The above elements suggest the placement of burden of managing an incident and threat reporting system on both the judicial branch and responsible law enforcement authority (i.e., the California Highway Patrol, Sheriff’s or local (court) Marshal’s office). The establishment of such a system should be codified in statute based on accompanying rules of court. An alternative, similar to the situation in Utah and the federal courts, would have contracted services for court security include a condition(s) which requires the reporting and/or recording of the incidents into a judiciary-based, automated incident reporting system. The best approach however still involves incorporating the current structure, mission, duties and responsibilities of

the CHIP, Sheriff's, and Marshal's. This can be effectively accomplished (i.e., maximizing existing resources) by enacting legislation in each of these specific areas of responsibility.

It is important to establish and maintain ongoing contacts and response protocols with law enforcement agencies at the local, state, and national level. These agencies can provide valuable information about those who may pose a risk to judicial officers. Connecting the dots that may link individuals or incidents together can serve to identify threats in a more timely fashion and, thereby, minimize the risk that such threats pose. To this end, regular communication, coordination and practice response with other agencies can provide vital assistance to those with responsibility for the safety and security of judicial officers.

VI. Conclusion

Working in today's court systems by its very nature is a risky business. Day in and day out, court buildings are visited by a large volume of disgruntled and even law-breaking citizens. Many of these individuals act out violence in their minds against judges and the courts they represent. As their hatred of the system builds, some release their anger by threatening certain judges with bodily harm or death in writing or by personal contact. It is a fact that federal and state court judicial officers can be seen as important symbolic targets for those in our midst who wish to wreak terror on the fundamental tenant of our constitution – the rule of law.

Providing safety and security to judges and to those who work in and visit courthouses is not a one time achievement. It is a serious and continuous goal and requires constant vigilance and increased communication between the object of the threat and those law enforcement agencies that are bound to protect them. Capturing, analyzing, and protecting against threats and incidents must be a number one priority, every single day for all those interested and involved in the process of protection. Although threats to judges and others in the judicial system can never be eliminated, they can be minimized with proper attention, action, and sharing of information in an organized manner.

APPENDICES

APPENDIX A
FEDERAL COURTS

COURT FACILITY INCIDENT REPORT

1. DATE OF REPORT _____	2. DATE OF INCIDENT _____	3. TIME OF INCIDENT _____																								
4. GSA BUILDING NO. _____	5. BUILDING NAME _____	6. BUILDING ADDRESS _____																								
7. ARREST/DETENTION <input type="checkbox"/> YES <input type="checkbox"/> NO	8. REPORTING DISTRICT _____	9. REPORTED BY _____																								
10. TYPE OF INCIDENT (<i>Check Applicable Box</i>) <table border="0"><tr><td><input type="checkbox"/> Alarm Activation</td><td><input type="checkbox"/> Medical Emergency</td><td><input type="checkbox"/> Suspicious Vehicles (Perimeter Areas)</td></tr><tr><td><input type="checkbox"/> Assault</td><td><input type="checkbox"/> Missing Property</td><td><input type="checkbox"/> Unauthorized Persons</td></tr><tr><td><input type="checkbox"/> Bomb Threat</td><td><input type="checkbox"/> Open/Unsecured doors</td><td><input type="checkbox"/> Vehicle Break-Ins/Burglaries</td></tr><tr><td><input type="checkbox"/> Contraband</td><td><input type="checkbox"/> Property Damage</td><td><input type="checkbox"/> Other (<i>Describe:</i>)</td></tr><tr><td><input type="checkbox"/> Disruptive Person</td><td><input type="checkbox"/> Security Breaches</td><td>_____</td></tr><tr><td><input type="checkbox"/> Forced Entry</td><td><input type="checkbox"/> Shooting</td><td></td></tr><tr><td><input type="checkbox"/> Illegal Weapon</td><td><input type="checkbox"/> Suspicious Individuals on Perimeter</td><td></td></tr><tr><td><input type="checkbox"/> Malfunctioning Equipment (alarms, elevators, garage doors, security lighting, etc.)</td><td><input type="checkbox"/> Suspicious/Unattended Package</td><td></td></tr></table>			<input type="checkbox"/> Alarm Activation	<input type="checkbox"/> Medical Emergency	<input type="checkbox"/> Suspicious Vehicles (Perimeter Areas)	<input type="checkbox"/> Assault	<input type="checkbox"/> Missing Property	<input type="checkbox"/> Unauthorized Persons	<input type="checkbox"/> Bomb Threat	<input type="checkbox"/> Open/Unsecured doors	<input type="checkbox"/> Vehicle Break-Ins/Burglaries	<input type="checkbox"/> Contraband	<input type="checkbox"/> Property Damage	<input type="checkbox"/> Other (<i>Describe:</i>)	<input type="checkbox"/> Disruptive Person	<input type="checkbox"/> Security Breaches	_____	<input type="checkbox"/> Forced Entry	<input type="checkbox"/> Shooting		<input type="checkbox"/> Illegal Weapon	<input type="checkbox"/> Suspicious Individuals on Perimeter		<input type="checkbox"/> Malfunctioning Equipment (alarms, elevators, garage doors, security lighting, etc.)	<input type="checkbox"/> Suspicious/Unattended Package	
<input type="checkbox"/> Alarm Activation	<input type="checkbox"/> Medical Emergency	<input type="checkbox"/> Suspicious Vehicles (Perimeter Areas)																								
<input type="checkbox"/> Assault	<input type="checkbox"/> Missing Property	<input type="checkbox"/> Unauthorized Persons																								
<input type="checkbox"/> Bomb Threat	<input type="checkbox"/> Open/Unsecured doors	<input type="checkbox"/> Vehicle Break-Ins/Burglaries																								
<input type="checkbox"/> Contraband	<input type="checkbox"/> Property Damage	<input type="checkbox"/> Other (<i>Describe:</i>)																								
<input type="checkbox"/> Disruptive Person	<input type="checkbox"/> Security Breaches	_____																								
<input type="checkbox"/> Forced Entry	<input type="checkbox"/> Shooting																									
<input type="checkbox"/> Illegal Weapon	<input type="checkbox"/> Suspicious Individuals on Perimeter																									
<input type="checkbox"/> Malfunctioning Equipment (alarms, elevators, garage doors, security lighting, etc.)	<input type="checkbox"/> Suspicious/Unattended Package																									
11. CHECK APPLICABLE BOX <input type="checkbox"/> INITIAL REPORT <input type="checkbox"/> FOLLOW-UP REPORT <input type="checkbox"/> ADDENDUM (initial report dated: _____)																										
12. INCIDENT DESCRIPTION (<i>Details should cover who, what, where, when and how.</i>) 																										
13. REPORT PAGES REPORT CONTINUED ON ____ ATTACHED PAGE(S).																										
<i>I hereby certify that the information stated herein is true, complete, and accurate to the best of my knowledge.</i>																										
14. SIGNATURE OF PREPARER _____	15. DATE _____	18. DISTRIBUTION DISTRICT COTR - 1 COPY OCS - 1 COPY																								
16. APPROVED BY: NAME _____ TITLE _____	17. DATE _____																									

COURT FACILITY INCIDENT REPORT

(Continuation Sheet)

1. DATE OF REPORT _____	2. DATE OF INCIDENT _____	3. PAGE(s) _____ OF _____
----------------------------	------------------------------	------------------------------

INCIDENT DESCRIPTION (Details should cover who, what, where, when and how.)

[Large empty rectangular area for incident description]

COURT FACILITY INCIDENT REPORT

BLOCK NUMBER	REPORT REQUIREMENT
1. DATE OF REPORT	State the date the report is being prepared.
2. DATE OF INCIDENT	Self explanatory.
3. TIME OF INCIDENT	Indicate the approximate time that the incident occurred.
4. GSA BUILDING NO.	Self explanatory.
5. BUILDING NAME	Self explanatory.
6. BUILDING ADDRESS	Self explanatory.
7. ARREST/DETENTION	Check the box at the bottom of this section if anyone is detained for any length of time or arrested.
8. REPORTING DISTRICT	Indicate the name of the district preparing the report. Please annotate if different than where the incident occurred.
9. REPORTED BY	Provide the name of person preparing the report.
10. TYPE OF INCIDENT	Check applicable box that best describes the type of incident. If "Other" is checked, give a one or two word description that best describes the incident.
11. CHECK APPLICABLE BOX	Indicate whether this is an initial report, a follow-up, or an addendum to a previous report.
12. INCIDENT DESCRIPTION	<p>At a minimum, the report must address the following:</p> <p>WHO: Provide the name(s) of the person(s) involved and their date of birth.</p> <p>WHAT: Describe what happened in detail.</p> <p>WHERE: Where did the incident happen? City, building, floor, room, etc.</p> <p>WHEN: Date and time of the incident.</p> <p>HOW: If not already covered in the "what" category, describe how the incident happened.</p> <p>All reports must be legible, complete, and accurate as possible. Explain the incident in detail, from the beginning to the end. Never end in the middle of the story.</p> <p>BE SURE THAT THE REPORT CAN BE READ BY SOMEONE OTHER THAN YOU.</p>
13. REPORT PAGES	If the narrative describing the incident is included on additional pages, write the number of pages attached. If contents of the report are sensitive in nature, each page should be marked "FOR OFFICIAL USE ONLY."
14. SIGNATURE OF PREPARER	Self explanatory.
15. DATE	Enter the date you signed this report.
16. APPROVED BY	Indicate the name and title of the Contractor's official reviewing and approving official.
	NOTE: The reviewing and approving official must be a supervisory representative.
17. DATE	Enter the date the report was reviewed, approved, and signed by the contractor's supervisory representative.
18. DISTRIBUTION	Immediately forward a copy of this report as indicated.

APPENDIX B
NEW JERSEY



NEW JERSEY JUDICIARY Incident Report Form

CHECK ONE: WORKPLACE VIOLENCE SECURITY

Fill Out If: you are a judiciary employee / manager or sheriff's officer.
When: you witness, are involved in, or are informed of a security incident such as a threat, assault, display or use of a weapon, escape from custody, theft, disorderly conduct, or disruptive behavior.
Where: in or around the courthouse, judiciary facility or other location where judicial programs operate, including parking areas, field locations and during official travel.
File Report: with immediate supervisor / manager, or Workplace Violence Liaison. **THIS IS A CONFIDENTIAL DOCUMENT.**

COURT / AGENCY / VICINAGE DATE OF INCIDENT TIME OF INCIDENT AM PM DAY OF THE WEEK

LOCATION / ADDRESS OF INCIDENT: STREET ADDRESS CITY

COURT HOUSE ANNEX COUNTY LEASED PARKING AREA STATE LEASED / OWNED OTHER COUNTY OWNED OTHER _____

COURT / AGENCY WHERE INCIDENT OCCURRED

CRIMINAL DIV. SPECIAL CIVIL COURT ADMIN. FAMILY DIV. MUNICIPAL COURT SUPREME COURT CIVIL DIV. TAX COURT

APPELLATE DIV. SHERIFF'S OFFICE PROBATION AOC SUPERIOR COURT CLERK'S OFFICE OTHER _____

AREA INCIDENT OCCURRED

ENTRANCE # _____ SCREENING POINT # _____ WAITING AREA # _____ PUBLIC HALLWAY # _____ ELEVATOR # _____ COURTROOM # _____ RESTRICTED AREA # _____

CHAMBERS # _____ CONFERENCE RM # _____ STAIRWELL # _____ OFFICE # _____ HOLDING CELL # _____ OTHER _____

TYPE OF INCIDENT

ASSAULT VERBAL THREAT MAIL THREAT DAMAGE / VANDALISM ESCAPE FROM CUSTODY DISORDERLY PHONE THREAT

BOMB THREAT THEFT FIRE ALARM OTHER (be specific) _____

WAS THERE AN EVACUATION? YES NO

INDIVIDUALS INVOLVED - Indicate: Subject (S) or Victim/Target (V)

DEFENDANT	—	—	PROBATIONER	—	—	JUDGE	—	—	JUDICIARY EMPLOYEE	—	—
PLAINTIFF	—	—	WITNESS	—	—	SHERIFF'S OFFICER	—	—	<input type="checkbox"/> CURRENT	<input type="checkbox"/> FORMER	
RELATIVE	—	—	ATTORNEY	—	—	TROOPER / GUARD	—	—	OTHER	—	—
SPECTATOR	—	—	JUROR	—	—	PROBATION OFFICER	—	—			

SECURITY VULNERABILITY INDICATED? (TO BE COMPLETED BY SHERIFF / AOC) SUBJECT ARRESTED / DETAINED?

YES NO YES NO

WEAPON USED, FOUND, DISPLAYED? IF YES, PLEASE DESCRIBE

YES NO

BRIEF DESCRIPTION OF INCIDENT

REPORT SUBMITTED BY: PRINT NAME: _____ SIGNATURE: _____	DATE	PHONE NUMBER
MUNICIPAL DIVISION MANAGER (IF APPLICABLE) PRINT NAME: _____ SIGNATURE: _____	DATE	COUNTY
WORKPLACE VIOLENCE LIAISON PRINT NAME: _____ SIGNATURE: _____	DATE	PHONE NUMBER

STOP! HAVE ALL QUESTIONS ON THIS FORM BEEN ANSWERED? YES NO

APPENDIX C
PENNSYLVANIA

UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

Security Incident Fact Sheet

CONFIDENTIAL

DISTRICT	02-1-01
DATE OF INCIDENT	March 18 2005
TIME OF INCIDENT	Hour Minutes a.m.

Check Boxes Only Where Applicable

WHAT WAS THE NATURE OF INCIDENT?:

You may choose multiple items from each area below.

You may enter another type of incident by typing a 2- or 3-word description in the "Other" box.

Personal		
<input type="checkbox"/> Disorderly Person(s)	Other (Describe below)	
<input type="checkbox"/> Physical Assault		
Threat		
<input type="checkbox"/> Bomb	Other (Describe below)	
<input type="checkbox"/> Suspicious Package		
<input type="checkbox"/> Verbal		
Threat Mode		
<input type="checkbox"/> Direct Contact		
<input type="checkbox"/> E-mail	Other (Describe below)	
<input type="checkbox"/> Mail		
<input type="checkbox"/> Telephone		
Property Damage		
<input type="checkbox"/> Arson	Other (Describe below)	
<input type="checkbox"/> Theft		
<input type="checkbox"/> Vandalism		
Drugs		
<input type="checkbox"/> Drugs or Contraband	Other (Describe below)	
Emergency		
<input type="checkbox"/> Contamination Exposure	<input type="checkbox"/> Medical	Other (Describe below)
<input type="checkbox"/> Explosion	<input type="checkbox"/> Prisoner Escape	
<input type="checkbox"/> Fire	<input type="checkbox"/> Weather	

WHAT WAS THE EXTENT OF INJURIES?:

- None
- Don't know
- Minor
- Medical attention required

Description of injuries:

WEAPON INVOLVED?:

You may choose multiple items and/or provide other description.

- None
- Box cutter
- Hands/feet
- Razor blade
- Biological agent
- Chemical agent
- Knife
- Rifle
- Blunt object
- Handgun/pistol
- Pepper spray
- Shotgun

Other: (Describe weapon(s) at right)

IN RELATION TO THE MAGISTERIAL DISTRICT JUDGE COURT FACILITY, WHERE DID THE INCIDENT OCCUR?:

You may choose multiple items and/or provide other description.

- Central Court
- Garage
- Grounds
- Staff area
- Chambers
- Hallway
- Lobby
- Courtroom
- Holding cell
- Parking lot

Off-site. Indicate address or location.
(Describe at right)

WAS AN ALARM ACTIVATED?:

- No
- Duress/Panic button
- Emergency call (911)
- Magnetometer/X-Ray

Other: What agencies were notified?

WHO WAS INVOLVED IN THE INCIDENT?:

You may choose multiple individuals and write in any not listed.

- Magisterial District Judge
- Prosecutor
- Security officer
- Defendant
- Court Staff
- Constable
- Sheriff
- Plaintiff
- Defense counsel
- Municipal police
- State police
- Prisoner
- Member of public

Other (Describe at right)

Were any of the persons involved in the incident attending a court proceeding? Yes No

If yes, what type of case?

- Civil Case Landlord/tenant Private Criminal Complaint Non-traffic Citation
 Criminal Case Protection From Abuse Traffic Citation

Case Caption (Enter at right)

If known, enter names of those involved. Enter number of names then click update.

SUMMARY OF FACTS:

Please include the name of each agency that responded to the incident (e.g., sheriff, state police, fire department) as well as the circumstances leading up to the event.

NAME OF INDIVIDUAL FILING THIS REPORT:

Did you personally witness the incident? Yes No

If you answered No above, enter the name of the person for whom you are filing this report:

Last name:

First name:

Middle initial:

Name suffix: (Jr., Sr.)

REPORT FILING OPTIONS

Save until I return and complete the report

(Allows you to return and edit this report within the next 7 days. This option is useful if you cannot complete the report at this time.)

OR

Save the report for the record

(This option will submit the report immediately. You will not have the option of editing this report at a later time.)

APPENDIX D

TEXAS



Texas Court Security Incident Report

- District, County and Justice Courts -
Texas Code of Criminal Procedure, Art. 102.017(f)

Form must be submitted not later than the 3rd business day after the date the incident occurred.

This form is for administrative purposes only. If law enforcement attention is needed, contact the local police or sheriff's department.

1. Information of Person Completing Form:
Last First Area Code and Phone
Title Email

2. Type of Court: District County Justice
Not related to a particular court type
Name of Court or Courthouse/Court Building:
3. County:
4. Incident Date: Time: AM PM

5. Type of Incident:
Physical assault Disorderly behavior
Bomb threat Hostage situation
Threat
Type of threat: Verbal Written
Threat against: Judge, judicial officer, court staff
Attorneys, witnesses, or jurors
Other:
Prisoner escape attempt
Attempt to bring a weapon into the courtroom or court building
Other:

9. Who was the perpetrator in the incident?
Name:
Criminal defendant/juvenile respondent
Plaintiff/non-criminal defendant/respondent/petitioner
Family member/friend of party in the case
Member of public (unknown relation to any case)
Other:
Was this individual charged as result of the incident?
No Yes Pending

6. Location of Incident:
Courtroom of: Judge Other judicial officer (associate judge, magistrate, etc.)
Chambers of: Judge Other judicial officer (associate judge, magistrate, etc.)
Staff offices of: Judge Other judicial officer (associate judge, magistrate, etc.)
Clerk's office
Holding area
Parking lot
Public area of courthouse/court building (lobby, hallway, etc.)
Other:

10. Was the incident reported to law enforcement?
No
Yes, name of agency:

7. Was a weapon involved?
No Yes, identify all weapons involved:
Gun Knife Blunt object
Other:

11. Was this incident related to a particular case within the court?
Criminal Civil Mental Health Not related to a particular case
Family Probate Juvenile
Case Number:
Style:

8. Was anyone injured?
No Yes, type of injury:
If yes, was medical attention rendered? No Yes

12. Description of Incident:
[Blank lines for description]

APPENDIX E

UTAH

This page has been formatted for printing.
Utah State Courts

Font size: A A A

Court Security Incident Form

Court Information	
District: All <input type="button" value="v"/>	Court Level: All <input type="button" value="v"/>
Location: All <input type="button" value="v"/>	

Incident Information	
Date of Incident: Jan <input type="button" value="v"/> 1 <input type="button" value="v"/> 2008 <input type="button" value="v"/>	Time of Incident: 1 <input type="button" value="v"/> 00 <input type="button" value="v"/> AM <input type="button" value="v"/>
Date of Incident Unknown <input type="checkbox"/>	Time of Incident Unknown <input type="checkbox"/>
Location of Incident: -- Select Incident Location -- <input type="button" value="v"/>	
Incident Type	
Personal	Property
<input type="checkbox"/> Assault	<input type="checkbox"/> Vandalism
<input type="checkbox"/> Fight	<input type="checkbox"/> Theft
	<input type="checkbox"/> Arson
Threat	<input type="checkbox"/> Trespassing
<input type="checkbox"/> Bomb	Illegal Substance
<input type="checkbox"/> Suspicious Package	<input type="checkbox"/> Drugs
<input type="checkbox"/> Personal	<input type="checkbox"/> Contraband
Threat Mode	Emergency
<input type="checkbox"/> Direct Contact	<input type="checkbox"/> Medical/Injury
<input type="checkbox"/> Telephone	<input type="checkbox"/> Prisoner Escape or Attempt
<input type="checkbox"/> Mail	<input type="checkbox"/> Fire
<input type="checkbox"/> Email	<input type="checkbox"/> Explosion
<input type="checkbox"/> Third Party	<input type="checkbox"/> Chemical/Biological Substance
<input type="checkbox"/> Possibly Gang Related	
<input type="checkbox"/> Other (describe) <input type="text"/>	

Victim Information			
Last Name:	First Name:	Age:	Gender: <input type="button" value="v"/>
<input type="checkbox"/> Check here if information is not known			
Relationship to Court: <input type="button" value="v"/>	Court Case Type: <input type="button" value="v"/>		

Injury:

Suspect Information

Last Name: First Name: Age: Gender:

Check here if information is not known

Relationship to Court: Weapon Used:

Narrative

Summary of facts.

Author

Name of Person Filing Report:

Did You Personally Witness the Incident? Yes No

Follow Up To be entered in by authorized personnel only.

Follow up information about this report.

Page Last Modified: 10/23/2008

APPENDIX F
WASHINGTON

INCIDENT REPORT FORM

(ANY form of threat or threatening actions that occur)

SECURITY REQUESTED ON:

Date: _____

Court Name: _____

“Incident” means a threat to or assault against the court or court community, including attorneys, court personnel, jurors, litigants, witnesses or others using the courthouse. It also includes any event or threatening situation that disrupts the court or compromises the safety of the court or the court community.

A security incident is not limited to a violation of law, but can include any act or circumstance that may interfere with the administration of justice. Examples include but are not limited to:

- Threats from the public
- Threats from an employee
- Disruptive behavior on court property
- Assaults, robberies, intimidation or threats to the court community either on or away from court property
- Assaults, robberies, intimidation or threats adjacent to the courthouse that affect access to the courthouse
- Work space quarrels between employees leading to acts of violence

SUMMARY OF INCIDENT

Date & time incident/threat occurred: _____

Location of Incident (*include Court name*) _____

If a threat occurred, was the threat made in person, or by letter, email or telephone?

Explain: _____

Your Name & Dept.: _____ Phone: _____

Names of witnesses and phone numbers, if available:

Describe what you observed happen/contents of any threats made. (If more space is required, use back of form.)

SUMMARY OF SECURITY/LAW ENFORCEMENT ACTION

Was Court Security or Law Enforcement contacted? YES NO

If so, what was the response? (i.e. called back, physically responded) _____

SUMMARY OF INJURIES

Was anyone injured? YES NO

If so, what action was taken? _____

SIGNATURE: _____ DATE: _____

E-mail form to: Courtsecurity@courts.wa.gov or FAX to: (360) 956-5700 Attn: Court Security



California State Court Security

Court Security Personnel Classification and Staffing Level Standards

Final Report – March 2012

Table of Contents

I.	Introduction	2-1
II.	Job Classifications and Staffing Levels Currently in Place in California	2-2
III.	Information Obtained from Jurisdictions Surveyed	2-6
IV.	NCSC Best Practices Guidelines	2-7
V.	Recommendations.....	2-12
VI.	Conclusion	2-13
	Appendices.....	A-2-14

I. Introduction

The National Center for State Courts (NCSC) was engaged by the Officer of Emergency Response and Security (OERS) within the California Administrative Office of the Courts (AOC), as the staff entity to the California Judicial Council, Court Emergency Response and Security Task Force, to address issues of classifications and staffing level standards for those personnel providing security services in courthouses. Security is currently provided in courthouses throughout the state of California by personnel of many varied classifications. These classifications include, for example, sworn peace officers, corrections officers, contract guards, and court attendants. In addition to the variances in classifications, there is little in the way of “staffing standards” in terms of how many officers need to be assigned to various security functions within a courthouse. According to OERS, there are no guidelines to clarify the classifications of personnel that should be used for these functions, and there is no benchmark on the minimum staffing necessary for each type of court security function. This makes it increasingly difficult for OERS to assist in designing optimal security staffing, personnel requirements, planning proposals and estimating budget requirements on new construction projects, courts and facility upgrades. Minimum standards are needed to provide for the planning and allocation of California court security funding.

To assist in addressing this problem, the AOC requested the NCSC make recommendations on a future approach for standardizing job classifications and staffing standards as follows:

- Review specific data collected by OERS and the AOC Finance Division on classifications currently used within the courts in California.
- Review other court systems nationally for trends, examples and consistent approaches to the primary security functions.
- Recommend a future approach to standardizing the court security classifications by job function and duty as well as minimum staffing needs for each function.

To address the issues posed by the AOC, the NCSC surveyed nine jurisdictions in order to gather information on classification and staffing levels for court security personnel. Due to requests for confidentiality jurisdictions are not identified in this part of the report, nor are they identified in Appendix 3-A:

Some of the jurisdictions surveyed are relatively comparable to California in size. For other jurisdictions, not relative in size to California, the NCSC has direct knowledge that the systems do work and have aspects that are commendable and can serve as models for other state court systems. It should be noted that in selecting jurisdictions to survey, the NCSC also focused on systems that were largely comparable to California in terms of courthouse security being provided by county sheriffs. There are other sorts of systems in place in a few other states. For example, the state of New York has a court-managed security system in which the vast majority of court security officers are employees of the court.

In addition to gathering information from the sample jurisdictions, the NCSC analyzed its own best practices guidelines for courthouse security in an effort to determine what might work best for California. These guidelines have been developed over the past several years as the NCSC has conducted security assessments of over 230 courthouses throughout the country. This report contains recommendations for an approach for California to standardize job classifications and staffing standards. The recommendations contained in this report are based on information gathered from the sample jurisdictions, as well as the NCSC's best practices guidelines.

II. Job Classifications and Staffing Levels Currently in Place in California

There are four general categories of personnel providing security services in courthouses throughout California.

- Sworn Peace Officers. These officers may be employed by the sheriff or court, per California Penal Code section 830.1. They are authorized to carry firearms. These officers are typically assigned for weapons screening oversight, criminal case bailiff duties, and transporting in-custody inmates within the courthouse.
- Non-sworn Public Officers. These officers are employed by the sheriff, per California Penal Code section 831.4. They may or may not be peace officers, and they may carry a firearm while on duty. These officers are typically assigned to provide holding cell security and weapons screening. They may be assigned to some bailiff duties in non-criminal cases.

- Civilian Court Employees. These employees work for the court, per California Government Code section 69921. They are not authorized to carry a firearm. They are typically assigned to civil courtrooms.
- Contract Security Officers. These officers are employed by third-party vendors under contract with the court or the sheriff. They are typically used to provide entryway weapons screening at courthouses.

Other than these four general categories, there are multiple job titles currently in use in California to describe court security personnel. The following Table A illustrates this plethora of job titles in use as of August 2011.

Table A

Job Titles	Explanation
Sworn Peace Officers	
<ul style="list-style-type: none"> • Deputy • Bailiff • Sergeant • Lieutenant • Captain • Commander 	In small and medium courts, a sergeant or lieutenant is typically in charge of court security. Larger courts may have a captain or commander. In some jurisdictions, the title of commander is given to other officers in charge of a division, and this designation may also be given to a lieutenant or captain. Courtroom bailiffs are typically sworn deputies.
Non-Sworn Sheriff Civilian Employees	
<ul style="list-style-type: none"> • Ranger Technicians • Ranger • Sheriff Security Attendant • Sheriff Special Officers Community Service Officer • Corrections Technician • Custody Assistants • Dispatcher 	These titles are typically used for duties other than courtroom bailiffs. These duties include entrance screening, control room operations, and interior and exterior patrols. They may also be used in the transportation and monitoring of in-custody defendants. These titles vary from one jurisdiction to another.
Other Titles	
Marshal	This title is utilized in two counties. Marshals are employees of the court, who provide security, bailiff, and transportation services.

Security Officer Contract/private security	The title of security officer may refer to a sheriff’s employee, court employee, or staff of a private contracted security service. Typically, private security officers are used at weapons screening stations.
Court Attendants	These are court employees, generally used as bailiffs in non-criminal court proceedings. Some courts use court attendants at entryway screening stations.

Not having standards or guidelines to help determine which security functions need to be assigned to what type of staff presents a problem. For example, which functions should be required to be assigned to an armed security officer who is a sworn peace officer? What functions can be reasonably performed by an unarmed civilian employee or contract staff?

In addition to the issue of classifications, there is no agreed upon set of standards or guidelines in California to determine staffing levels for each functional area. Such standards might cover, for example, how many officers should be assigned to each entry screening station, or how many for each courtroom depending of case type. The following summary suggestions for staffing level issues were developed by OERS:

- Number of screeners varies with volume
- At least one bailiff in each courtroom
- Holding area and transport – varies
- Control room – should be staffed during all business hours
- Supervision – varies on staff size
- Administration – one position to ensure paperwork is submitted on a regular basis

The absence of staffing level standards throughout the state is reflected in the disparity in the number of security personnel from county to county. Table B below sets forth the relationship of the number of security personnel to annual filings for all counties in California with superior court annual filings of 230,000 or more. As the table indicates, this relationship varies from a low of 1762 filings to a high of 3141 filings for each security FTE.

Table B

County	Superior Court Filings FY 2009	Filings/Security FTE
Los Angeles	2,998,791	1950
Orange	741,935	2147
Riverside	565,162	3141
San Bernardino	629,037	2603
San Diego	760,757	2685
Alameda	444,705	2424
Contra Costa	215,390	2368
Fresno	242,928	2116
Kern	255,542	2696
Sacramento	417,150	2428
San Francisco	233,289	2758
San Joaquin	206,383	2971
Santa Clara	368,245	1762
Ventura	223,569	2849

There may well be other factors that help to explain the variances indicated in Table B. The mix of case type (e.g., civil, criminal, family, etc.) and the nature of the populations served by the court (e.g., the presence of juvenile gangs) are but two of such possible factors. Nonetheless, once other factors are taken into account, it is reasonable to look for a relatively consistent correlation between the amounts of business conducted in a court, as evidenced by the filings, and the number of personnel required to provide security for that court. Security staffing standards or guidelines would serve to foster that consistent correlation.

Table C below lists a sample of courts that lack uniform staffing standards. These court locations are scheduled to move into new facilities. Table C looks at the ratio of the number of security personnel assigned compared to certain workload indicators that would drive the need for security staff. These workload indicators include number of screening stations, number of courtrooms, number of buildings, etc. Column A displays the number of security FTE currently assigned per one workload indicator. There is a wide variance in these numbers, ranging from a low of 0.5 FTE in Fresno Sisk to a high of 1.7 FTE in Contra Costa East. Column B indicates the new staffing levels proposed by OERS, resulting in less of a variance, with the courts in San Benito and Calaveras coming more into line with the other locations. As with the data in Table B, other factors may explain the variances in the ratios set forth in Table C. Although a variance

will always exist, there should be some level of consistency. Column B does reflect that OERS is taking reasonable steps to foster consistency with respect to these particular court locations.

Table C

County	<u>A</u> Ratio of <u>current</u> security FTE to workload indicators	<u>B</u> Ratio of <u>proposed</u> security FTE to workload indicators
Santa Clara	1.4	1.6
Contra Costa East	1.7	1.7
San Benito	0.7	1.7
San Bernardino	1.9	1.9
Calaveras	0.6	1.3
Fresno-Sisk	0.5	0.6
Lassen-Susanville	1.1	1.1

III. Information Obtained from Jurisdictions Surveyed

The jurisdictions surveyed for this report revealed very little in the way of hard and fast rules for assignment. There are many approaches that jurisdictions can and do take with respect to security staffing in courthouses. Nonetheless, information gathered from the jurisdictions sampled offers the following general observations with respect to both classification and staffing level guidelines.

- A. One overall classification of a law enforcement officer, with arrest powers and the authority to carry a firearm exists in all of the jurisdictions surveyed. Typically this officer is a sheriff deputy, a municipal police officer or an officer employed by the court. In most of the jurisdictions surveyed, there is a second classification of security officers, used primarily to staff entry screening stations. This second level of classification is typically not a sworn officer. These screening officers may be employees of the court or employees of private security firms on contract with the court or sheriff department.
- B. The jurisdictions surveyed do not have published standards or guidelines on staffing levels. Staffing levels for security personnel is usually dependent on budgets and the

volume of courthouse traffic. The following, however, is generally true for these jurisdictions:

1. Usually two to three officers are assigned to each screening station. There may be more in larger urban courts, and fewer in smaller rural court settings.
2. At least one security officer is assigned to a courtroom while court is in session; more are assigned as conditions warrant.
3. If there is a command and control center, it is typically staffed by one full time security officer.
4. There are great variances in terms of the number of transport officers assigned to escort in-custody defendants.
5. Security patrols in the interior and exterior of the courthouse are conducted only as security officers have time and/or the inclination to do so.

More details of the observations derived from the surveyed jurisdictions can be found in Appendix A.

IV. NCSC Best Practices Guidelines

The NCSC has published best practices guidelines for courthouse security. These guidelines were developed by a group of security experts, who on behalf of the NCSC have conducted security assessments over the past several years on over 230 courthouses across the nation. The guidelines include information on classification and staffing levels for personnel providing security services to courthouses.

With respect to classification, the best practices guidelines recommend that an officer providing security in a courthouse, referred to as a court security officer (CSO), should be an individual trained in court security and certified to use a firearm. The CSO should be armed with a firearm, using a triple-retention holster. Note: As feasible, the CSO could be a sworn peace officer with statutory powers of arrest.

In terms of staffing levels, the best practices guidelines recommend the assignment of security staff by functional areas. It is estimated that each assignment requires 1.33 FTE to cover for sick and annual leave and training. Recognizing that implementing these best practices guidelines can be costly, the NCSC has developed steps in phases. By taking these steps, courts in their discretion can adopt incremental improvements before reaching the level of best practices. This is particularly important for a state like California that faces considerable

budgetary challenges. California, given its budgetary constraints, can focus on taking steps until such time as budgets and other factors permit it to achieve best practices. As discussed more fully below (see discussion around Table D), jurisdictions surveyed for this report have achieved levels of staffing consistent with the steps approach advocated by the NCSC. Prior to discussing the steps, the following are the best practices themselves.

Screening station: Assign three CSOs to operate the public entryway 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 such as external patrols and internal building walk arounds. Ideally, all three CSOs should be armed using a triple-retention holster, but at least one should be armed at all times. If two or more public screening stations are in operation, a fourth CSO should be assigned as a supervisor to oversee operations.

Courtrooms: Two CSOs should be assigned to a courtroom whenever any criminal court hearing is being held; one CSO should be assigned to protect the judge and one to watch courtroom activity. A third CSO (or transport officer) should be assigned when there is an in-custody defendant present. An additional CSO should be assigned when an in-custody criminal jury trial is being held; one to protect the judge, one for the jury, one to guard the in-custody defendant, and one to watch the spectators and entryway to the courtroom. Usually only one CSO should be assigned for any civil hearing or civil jury trial. However, a second CSO could be assigned based on the risk involved in a particular civil case, e.g., mental health, termination of parental rights. For criminal and civil high-visibility trials or volatile hearings an additional CSO should be assigned to the courtroom.

Command and control center: Establish a command and control center in a secured area of the court building and assign CSOs. For smaller court buildings, the monitoring function of a command and control center can take place in proximity to the front entrance screening station. Provide additional security personnel as required to supervise and monitor command and control center activities. CSOs should rotate monitoring screens approximately every 45 minutes to avoid *snow blindness*, i.e., inability to focus on images on monitors.

After-hours access: 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.

Conduct a full screening requiring everyone to go through the magnetometer and x-ray station. As time permits, the CSO should periodically patrol the interior and exterior of the court building.

Escorting in-custody defendants: Assign at least two CSOs or transport deputies to escort in-custody defendants through chambers hallway or other public areas, with one to clear the path ahead. The transport officer having physical contact with the prisoner should be unarmed; the other officer should be armed and remain a safe distance behind the transport.

Jurors: Assign a CSO to protect the jury room or clerk's office whenever juror payment is being made and when juror funds are obtained and transported back and forth in and out of the court building. Assign a CSO to provide security inside and outside the jury assembly room when potential jurors are present. Assign a CSO to escort jurors to and from the courtroom. If jurors who are serving on a jury trial are dining as a group outside the court building, a CSO should accompany them. If an elevator is used to transport jurors, one CSO should supervise the loading of jurors and another CSO should meet the jurors on the floor on which they disembark. Assign a CSO to remain with the jury during and after the entire trial/deliberation. Note: Additional protection for jurors could be provided after a high visibility trial has concluded and as jurors leave the court building to their mode of transportation.

Judges parking: Judges (and court staff) should be escorted to the unprotected parking lot by a CSO when they leave the court building late at night. Judges and court staff should be escorted to their cars or other mode of transportation after business hours. 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.

Patrols: Provide regular security patrols by CSOs at the public counters. Require two people – one court staff and an armed CSO – when carrying cash outside the court building. Note: A preferred procedure is for the court to use an armored car service to pick up daily deposits. Require scheduled patrols of all interior and exterior areas 24/7, either by CSOs or local law enforcement officers.

The NCSC best practices guidelines also emphasize the important issue of training for security personnel. 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. All CSOs should receive at least 16 hours of mandatory in-service training on court security each year. In addition to requiring 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. Note: Pre-service law enforcement academy training is usually required.

As indicated above, recognizing that implementing these best practices guidelines can be costly, the NCSC has developed steps in phases that can be taken with the goal of ultimately achieving best practices. By taking these steps, courts in their 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 the NCSC recommends that courts achieve over time. 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. The NCSC steps to best practices for security staff are attached as Appendix 3-B to this report. The complete document, *Steps to Best Practices*, is available on the NCSC website at www.ncsc.org.

It is useful to correlate the recommendations in the *Steps* document with the staffing levels found in the jurisdictions surveyed for this report. This correlation is set forth in the following Table D.

Table D

Staffing Levels in Sample Jurisdictions	Recommendations in the <i>Steps</i> Document
<p>Usually two to three officers are assigned to each screening station. There may be more in larger urban courts, and fewer in smaller rural court settings.</p>	<p>Topic B-1 of <i>Steps</i> deals with screening stations. As with all the topics in the <i>Steps</i> document, there is a “pathway” provided for courts to achieve best practices. Step 3 of Topic B-1 calls for one officer to staff the screening station. Step 13 calls for a second officer. Step 22 calls for a third officer. All in all, there are 27 recommended steps that courts can take in achieving best practices for screening stations in accordance with Topic B-1. Staffing levels are only one of the factors that courts need to take into account in this topic.</p>
<p>At least one security officer is assigned to a courtroom while court is in session; more are assigned as conditions warrant.</p>	<p>Topic B-4 addresses courtroom security. Step 1 calls for one officer to be assigned to each floor that has one or more courtrooms. Step 10 calls for one officer to be present in a courtroom whenever there is any proceeding in the courtroom. Step 14 calls for a second officer to be assigned in the courtroom (but not ordinarily for a civil case unless specifically requested by a judge). Step 18 calls for an additional officer for a high-visibility trial. All in all, there are 23 recommended steps that courts can take in achieving best practices for courtroom security in accordance with Topic B-4. Staffing levels are only one of the factors that courts need to take into account in this topic.</p>
<p>If there is a command and control center, it is typically staffed by one full time security officer.</p>	<p>Topic A-1 addresses command and control centers. Step 1 calls for one officer to be assigned to the center. Step 6 calls for additional officers to be added as required for effective monitoring.</p>
<p>There are great variances in terms of the number of transport officers assigned to escort in-custody defendants.</p>	<p>Topic B-8 addresses handling of in-custody defendants. Step 1 calls for one officer to escort in-custody defendant(s). Step 5 calls for a second officer to escort in-custody defendants. There is no specific ratio of defendants to officers recommended in <i>Steps</i>.</p>
<p>Security patrols in the interior and exterior of the courthouse are conducted only as security officers have time to do so.</p>	<p>Topic D-2 addresses interior and exterior patrols. The steps in this topic call for regular and random patrols.</p>

A careful review of the *Steps* document will lead the reader to understand that the recommended best practices are aspirational and that there are many steps along the way that can

be taken to achieve the recommended goals over time. Budgets are a reality, and in the current environment, budgets are becoming ever more constraining. Courts should strive to move as far along the *Steps* pathway as they reasonably are able, given present day budget constraints. As Table D indicates, courts in the sample jurisdictions appear to have staffing levels that are reasonably consistent with the recommendations contained in the *Steps* document. They may not have achieved the best practices level, but they are on the pathway to these aspirational goals.

V. Recommendations

Given the current structure for security personnel in California, the NCSC recommends that the Judicial Council work with the sheriff departments throughout the state to establish a pathway toward a higher level of standardization in terms of both classification and staffing levels. With respect to classification, a reasonable and achievable goal is that the classification of sheriff deputy could serve in all areas of courthouse security, with the exception of screening stations. Unarmed guards could staff entry screening stations under the guidance of at least one armed deputy. This two-tier approach appears to be working well in the jurisdictions surveyed and is consistent with the NCSC best practices guidelines. This structure already exists in many California court locations. Migrating toward more statewide consistency with this two-level approach will make for a more predictable and manageable system for the California court system.

It is possible that migrating toward the two-level approach may entail additional costs with respect to specific classifications currently in use in California. A detailed compensation and classification study will be needed to support the recommended migration. Such a study can serve to steer an overall approach in a manner that is cost-efficient, or at least cost-neutral.

With respect to staffing levels, the information gathered from the jurisdictions surveyed indicates that rigid staffing standards are generally not in place or rigorously adhered to. Budget vagaries and operational complexities make it difficult to adopt and implement firm staffing standards. Notwithstanding the difficulties and challenges, it is extremely important for California to strive to put staffing standards into place, working with sheriff departments throughout the state. Moving toward standardization will allow the state to pursue necessary consistency in security from courthouse to courthouse, and to engage in meaningful planning for

new and remodeled courthouses. More standardization may in the long run provide the most cost-effective means for doing so. The NCSC best practices guidelines can serve as a useful framework for the California courts to address staffing standards. The AOC should adopt the NCSC best practices guidelines as an aspirational goal. The “steps” approach to best practices, as set forth in Appendix B, provides a realistic means of achieving that goal over time.

VI. Conclusion

Given the current disparity on classifications and staffing levels for security personnel in courts throughout California, it is a daunting challenge for OERS and the Judicial Council to move toward a greater degree of standardization in these areas. However, the opportunity exists to work with sheriff offices in the state toward realizing this goal. The recommendations contained in this report provide a framework for establishing and pursuing a goal of more standardization, which in the end will serve to provide a more consistent level of courthouse security in the state.

APPENDICES

Appendix A
Information from Nine Sample Jurisdictions

Classification	Staffing Levels
Jurisdiction #1	
Entry Screening Stations	
<p>In Jurisdiction #1, screening officers (bailiffs) are employed by the court system for one level of courts in the state. There is a lead bailiff in each courthouse and a supervising bailiff in most (larger) districts. Bailiffs have firearms and are required to get a special permit from the state police. Bailiffs have full police powers when on court property. They receive a “special police commission.” This comes from the Secretary of State on behalf of the Governor. It must be renewed every three years.</p> <p>There are no specific education qualifications for bailiffs, other than a high school diploma. For experience, bailiffs need to have been a police officer for at least two years and have graduated from a police academy. On an informal basis, the court wants the police experience to be relatively recent. Bailiffs are almost exclusively former police officers. Training is mostly on the job.</p>	<p>Typically, two bailiffs at each station</p>
Courtrooms	
<p>The same classification – bailiffs – is used for courtroom security.</p>	<p>One bailiff assigned to all regular courtrooms. Two bailiffs are assigned to so-called “enhanced” courtrooms. This is a special program for larger districts in the state.</p>

Other Functions	
<p>Sheriff deputies are in charge of holding cells, and various law-enforcement agencies have responsibility for transporting in-custody defendants to, from, and within courthouses. Bailiffs perform interior patrols, and to a lesser extent, exterior patrols. Where there are other government agencies located in the courthouse, a state agency will use unarmed contract guards to conduct exterior patrols and provide after-hours security.</p>	<p>There are no statewide staffing standards for these functions. Assignments may be driven by budget more than by strict standards. To the extent standards exist, they would vary from county to county.</p>
Jurisdiction #2	
Entry Screening Stations	
<p>In Jurisdiction #2, the screening stations are staffed and operated by contract security screeners who are employees of a private contractor. Screeners are uniformed but unarmed.</p>	<p>The numbers of screening officers assigned will vary from location to location. In the largest city within this jurisdiction, there are between two and four officers assigned to each station.</p>
Courtrooms	
<p>Other than screening stations, security is provided by deputy sheriffs.</p>	<p>As a general rule, there is no armed security presence in a courtroom when court is in session. The only exception is in the arraignment courtroom where one deputy sheriff is permanently assigned. In all other courtrooms, a transport officer is present when an in-custody defendant is in the courtroom. A judge may on occasion request the presence of one or more armed deputies if the judge believes that it is warranted.</p>
Other Functions	
<p>Other than screening stations, security is provided by deputy sheriffs. Deputies serving as transport officers may or may not use weapons, depending on the situation. Deputies are armed and are sworn peace officers. Hiring at the entry level requires graduation from high school, or equivalent and at least one year of general work experience.</p>	<p>Exterior and interior patrols are conducted as resources are available. Prospective jurors are not tightly supervised, but are allowed to wander on their own inside the courthouse. There is no deputy assigned to the juror assembly area. Once individuals are assigned to a jury, they receive a juror badge and are accompanied by a law clerk/bailiff. There is a 5 to 2 ratio for escorting in-custody defendants. That is, for every five in-custody defendants, two deputies are assigned. For every additional defendant over five a 5 to 1 ratio is used.</p>
Jurisdiction #3	

Entry Screening Stations	
<p>As a general rule in Jurisdiction #3, sheriff deputies staff screening stations. In two or three counties, sheriffs have supplemental officers at screening stations (called security officers or security guards). These security officers or guards are not sworn law enforcement officers. In perhaps one or two counties, two sheriffs have contract guards (in one case armed, in the other case unarmed).</p>	<p>Staffing levels at screening stations vary by county. Staffing may depend on volume. Typically, there are three officers assigned to a station that may include an x-ray machine and a magnetometer (plus a second magnetometer at some stations).</p>
Courtrooms	
<p>Sheriff deputies provide security in courtrooms. All sheriff deputies are sworn law enforcement officers. All go through an academy.</p>	<p>At least one deputy in each courtroom. At least two deputies in each criminal courtroom, plus transport officers for in-custody defendants.</p>
Other Functions	
<p>Sometimes jail officers will hand off the prisoners to deputies. The courts deal only with deputies.</p>	<p>Typically two deputies are assigned for each in-custody defendant, but it varies by county. Normally one deputy is assigned to a jury after it is empaneled. Interior and exterior patrols are conducted based on staff availability.</p>
Jurisdiction #4	
Entry Screening Stations	
<p>In Jurisdiction #4, screening is conducted by CSOs who are employees of the court. There is one level of CSO, supervisors, managers, a deputy and a director. CSOs have no firearms; some have Tasers. CSOs do not have peace officer status or arrest powers. The education requirement for a new-hire CSO is a high school diploma or GED. If new CSOs have experience, it is considered a plus. New CSOs without experience are never initially assigned to a one or two man post and always get mentored. There is a three week training course, plus 30 hours of in-service training, to include, for example, CPR, tactics, x-ray, customer service. Perhaps 25% of the CSO force consists of retired police officers and retired military.</p>	<p>There are one to three CSOs assigned to a screening station, depending on volume and amount of equipment. Usually there are three CSOs assigned if the station has a magnetometer and x-ray machine. More CSOs may be assigned at a larger station.</p>
Courtrooms	

<p>Sheriff deputies have responsibility for courtroom security (on a case by case basis). Deputies are armed and are sworn police officers with arrest powers.</p>	<p>There is an armed deputy assigned to any case determined to be a security risk. This is done on a case by case basis. There will be a transport officer assigned if there is an in-custody defendant involved.</p>
<p>Other Functions</p>	
<p>Sheriff deputies have responsibility for courthouse security. Deputies are armed and are sworn police officers with arrest powers. There are transportation sheriff deputies who escort in-custody defendants to and from courtrooms and remain in court with the defendant. Transport deputies are never armed (they may have a baton). There is the same classification for transport and regular deputies. Jurors are guarded by a civilian bailiff or by a deputy only if there is a known threat. Deputies have more extensive training than CSOs, six to nine months before assignment to official duty.</p>	<p>Deputies regularly patrol the exterior and interior of the courthouse as staff is available. There is a CSO in the command and control center on a 24/7 basis.</p>
<p>Jurisdiction #5</p>	
<p>Entry Screening Stations</p>	
<p>In Jurisdiction #5, screening is provided by the municipal police department. Staffing at the screening station consists of uniformed officers who are armed and have full arrest powers. The stations are also staffed by civilian employees of the police department. These employees are unarmed and wear a blue blazer.</p>	<p>There is always at least one uniformed and armed officer present at each screening station, sometimes more. There is typically one civilian employee as well. There is a uniformed sergeant who serves as the supervisor.</p>
<p>Courtrooms</p>	
<p>Sheriff deputies provide security in the courtrooms. Sheriff deputies are post-certified and uniformed, but are not armed. Only the captain and sergeant are armed.</p>	<p>There is always one deputy present when the judge is on the bench. If there is a felony trial with in-custody defendant(s), there is one or more transport officers present as well. High-profile trials will have additional deputies assigned. Police officers will generally appear when a verdict is read in a high visibility trial, or in any trial that may warrant additional security.</p>

Other Functions	
Civilian police employees staff the command and control center. Deputies escort jury panels. Police officers do interior and exterior patrols. Transport officers do not carry firearms (but they do carry pepper spray).	There is typically one civilian police employee in the command and control center. Police do patrols as staff is available. Deputies will also “walk the halls” as they have time.
Jurisdiction #6	
Entry Screening Stations	
There is much variation from location to location in Jurisdiction #6. In its largest circuit court, a private security firm does entry screening. Screening staff are unarmed. The only training is whatever is required for private security guards. They report to court operations managers.	No standards. Vary from county to county.
Courtrooms	
Judges have bailiffs or CSOs. They are retired law enforcement officers, who have to maintain basic requirements. They are armed and have police powers. CSOs are authorized to carry weapons. Some do not carry per their judge’s directions. CSOs, if hired exclusively as court officers, require a minimum 120 hour training course. Approximately 75% of CSOs are qualified as full-time police officers and have undergone 12 week training at the state police academy. If not certified as a police officer, CSOs have a year to get the 120 hour training course. Then they have police officer status only while on duty in the courthouse. 80% of CSOs are retired police officers.	Varies, but typically at least one in each courtroom.
Other Functions	
Sherriff deputies transport in-custody defendants from the outside into courthouse detention centers, and then to courtrooms. On a case by case basis, deputies may give over custody to bailiff/CSO, or not. CSOs guard jurors. Deputies patrol inside and outside.	Deputies patrol inside and outside. No prescribed patrols. They are conducted as staff is available.
Jurisdiction #7	

Entry Screening Stations	
In Jurisdiction #7, there is a large force of court officers who provide security to courts throughout the state. Less than 10% of the state use sheriff deputies for court security. Court officers handle entry screening, courtrooms, and all other functions. Titles for court officers are: court officer trainee (for two years); court officer; sergeant; lieutenant; captain; major; assistant chief; deputy chief; and chief. The entry level education requirement is a high school diploma. There is no specific experience requirement. Court officers carry weapons. They have peace officer status and arrest powers. Officers enroll in a 14 week pre-service academy and are provided ongoing in-service training.	Ideally two court officers are assigned to a screening station that has a magnetometer only. Three officers are assigned to a station that has both a magnetometer and x-ray machine. These numbers will vary with screening station volume. They also may be affected by budget constraints.
Courtrooms	
See above under Entry Screening Stations.	The number of court officers assigned to courtrooms will range from five officers assigned for an arraignment courtroom to one officer assigned to a civil courtroom.
Other Functions	
See above under Entry Screening Stations.	For escorting in-custody defendants they try to assign two court officers for one defendant. There is never less than a 1:1 ratio.
Jurisdiction #8	
Entry Screening Stations	
Varies with sheriff departments, from county to county. Some counties have contract or civilian screeners.	Varies with sheriff departments, from county to county.
Courtrooms	
Varies with sheriff departments, from county to county.	Varies with sheriff departments, from county to county.
Other Functions	
Varies with sheriff departments, from county to county.	Varies with sheriff departments, from county to county.

Jurisdiction #9	
Entry Screening Stations	
Contract Court Security Officers (CSO) handle screening operations. CSO Qualification Standards: U. S. Citizenship, at least 21 years of age, high school graduate, English language fluency, valid state driver’s license with a five-year safe driving record, three years certified law enforcement experience.	Minimum of two (2) CSOs provide screening per screening station (one on the x-ray, one on the walk through metal detector). During busier times (early morning and after lunch) a third CSO may be assigned to assist.
Courtrooms	
Contract CSOs provide security during some courtroom proceedings. However, all in-custody defendants are handled and secured by deputies. In courtrooms, CSOs maintain order and security while deputies provide protective services for judges and handle prisoners.	Usually one CSO per courtroom when covered. This CSO is pulled from the Roving position.
Other Functions	
CSOs provide roving patrols inside courthouses, with an allocation of one CSO for every two floors of a courthouse. CSOs monitor the security of the courthouse via CCTV in a control room and will also cover such ancillary posts as access control to judiciary parking, employee entrances to verify employee IDs, exterior patrols to assure that no suspicious packages are left near the building.	The number of CSOs allocated to a specific facility is based on a formula that takes into account the hours of court operations, number of floors occupied by court operations, the number of judges assigned to a specific courthouse as well as other security needs.

Appendix B

Steps to Best Practices for Court Security Personnel

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-4: COURTROOMS

Phase One

1. Assign at least one CSO on every floor that has one or more courtrooms, dedicated as a “rover” from one courtroom to the next (unless local or state rules require additional coverage). There must be at least one CSO or transport officer present throughout the entire court proceeding whenever an in-custody defendant is involved.
2. Install duress alarms in the courtroom at accessible locations:
 - On top or under the working surface of the bench, plainly marked
 - At the CSO station
 - At the clerk’s stationTrain judges and staff on the functionality of duress alarms and on the protocols for use.
3. Test duress alarms regularly (at least monthly).
4. Conduct a sweep in the morning before a proceeding is held and at the end of the day for all trials to court and trials to jury. (For high visibility trials, use a dog trained with the ability to detect guns, bomb materials, and other explosive contraband.)
5. Secure or remove all metal and glass items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, glasses). As substitutes for these items use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers.
6. Install and then regularly test emergency lighting/fire equipment in courtrooms.
7. Always keep front and back doors to courtrooms locked when courtroom is not in use.
8. Use proper and acceptable restraints per state law on in-custody defendants.
9. Prohibit use of camera/cell phones in the courtroom and prohibit other items that could be used as weapons.

Phase Two

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

10. Assign at least one CSO to be present in the courtroom whenever there is any court proceeding being held in 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-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 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.



California State Court Security

Court Security Plans

Final Report – February 2012

Table of Contents

I.	Introduction.....	3-1
II.	Overview of Selected States Security Plans	3-1
III.	Review of Security Plan Subject Area Requirements.....	3-9
IV.	Recommendations for California Rule of Court 10.172 and for Improving Security Plan Compliance in Local Courts.....	3-11

I. Introduction

Every person who attends a court proceeding or is present in a court facility is entitled to a safe and secure environment. A court security plan establishes policies and procedures to be followed by security and court personnel in order to prevent and respond to court security incidents. The presence of a court security plan is integral to the safety of the courthouse; therefore, many states have adopted statutes and/or court rules requiring that all courts complete their own plan. California has adopted such a rule and is making strides to increase compliance to the rule among its local courts. The intent of this report is to present information to California from other states which have adopted court security plan requirements and to make recommendations to California for improving its rule of court and developing strategies for improving compliance among trial courts.

For this report the National Center for State Courts (NCSC) reviewed the California Rule of Court 10.172 as well as statutory and court rule requirements of five other states including Arkansas, New Jersey, Ohio, Oregon and Utah. To understand the implementation of the various court rule requirements, the NCSC reviewed specific administrative policies, techniques and governance structures for the purpose of understanding successful best practices. In California, for instance, the state's online security plan template was reviewed because it is a primary tool the AOC has in place for helping local courts to complete their security plans.

In reviewing the other states, the NCSC conducted interviews with senior state court security officials and collected relevant supporting security planning materials from the aforementioned states regarding their practices and tools used for gaining compliance that may be considered by the California Judicial Council. The NCSC's findings are presented within the body of the following report and relevant supporting materials are presented in the appendices.

II. Overview of Selected States Security Plans

Arkansas

Arkansas is a unified court system which includes appellate courts, circuit courts, district courts and city courts. The implementation of a statewide court security plan in Arkansas has gained considerable traction in the last five years. In 2005 a State Court Security Task Force was

convened and ultimately developed a series of recommendations regarding court security in Arkansas. Out of these recommendations came legislation in 2007 which established a State Security Committee, a Director of Security and Emergency Preparedness and a number of security and emergency preparation recommendations (not requirements), including the recommendation that all counties complete a court security plan, an emergency response plan, and a continuity of operations (COOP) plan for all court facilities in their jurisdiction.

The State Security and Emergency Preparedness Advisory Committee, created in 2007, has 17 members including two state legislators and representatives from police and sheriff law enforcement agencies, county government, county prosecuting and defense attorneys, judges and court administrators. The Committee was created by the legislature for the purpose of recommending and evaluating uniform state policies on court security. The committee has the authority to recommend future legislation regarding state court security and emergency preparedness. The Director of Security and Emergency Preparedness, overseen by the State Security Committee, provides direct assistance to the state's circuit courts (general jurisdiction) and district courts (limited jurisdiction,¹ in implementing their security plans and serves as the point of contact on issues of security and emergency preparedness for the judicial branch.

The legislation in 2007 did not explicitly require that all courts complete a security plan but did set up a monetary framework for getting local courts to comply with recommendations (i.e., development of a court security plan). The legislation included the creation of a State Court Security Grant fund controlled by the State Security Committee. In effect, for counties to be eligible for security funding grants, they must make a good faith effort to develop a security plan using the guidelines and templates established by the Court Security Director.

In Arkansas, the first step of a court security plan is completing an assessment to determine where the vulnerabilities and strengths are. In developing the plan, a county must show that it has addressed known security issues or vulnerabilities illustrated in the assessment. For example, "Have you minimized the number of building entrances?" "Do you have duress alarms and are they tested?" "What type of training is available for security officers?" "Do you

¹ Arkansas is currently in the process of consolidating local City Municipal Courts with State District Courts and it is expected that this process will continue over the next several years. (As of November 2010, 13 counties have merged their City Courts into District Courts.) Eventually all city courts will be merged into District Court jurisdiction. The District Courts may or may not maintain the same existing facilities.

have an emergency backup generator? If not, what are your plans to address this issue?” Counties completing a security plan do not have to solve all of their problems to be eligible for grant monies; instead, they must show that they have addressed the problems.

It is recommended that a security plan be submitted annually, but there are no sanctions for non-compliance. For non-compliers, it is up to the State Security Director to approach individual courts and ask if plans have changed. If plans are not up to date, then the AOC may withhold eligibility for grant funds. The State Security Office offers assistance to counties in helping complete their plans.

The state does not have 100% compliance in completing security plans. Out of 75 counties, 48 are 100% compliant with all three types of plans; 56 counties have done some of the plans. The Office of Security is hopeful that in the next few years the state will have 100% compliance as all non-compliers have indicated that they want to complete their plans.

New Jersey

New Jersey is a unified state court system which has significantly enhanced its security programs over the last several years. The state has 21 vicinages encompassing 114 state court facilities and 537 municipal courts. State statute mandates that county sheriffs provide security in a manner decided by the assignment judge of each court. An AOC mandate requires that all courts establish and maintain a security committee and local security plan. Local court security plans are modeled after the state’s Model Court Security Plan which was first developed by the AOC in 2001 and revised in 2006. In 2006 the AOC sent out a directive for courts to come into compliance with basic security protocols such as universal weapons screening and officers in the courtroom.

As part of the model court security plan, every court in the state is required to complete an annual self-audit risk assessment and physical security survey. Security for each court is then specifically tailored to the risk assessment. In addition, each court is required to complete an external security audit every two years.

The state did not have good compliance from local courts in completing local security plans until 2006, especially at the municipal court level. The impetus to achieve more universal

compliance came after a large number of security incidents occurred in 2005 at which point awareness of security vulnerabilities was heightened and a task force was convened to address the issue. The task force included three assignment judges and three sheriffs and resulted in the revised model court security plan and the recommendation that the Model Court Security Plan be implemented in all courts. Soon after, the State Court Administrator approved the recommendations and ordered a timeframe for all courts to complete a local court security plan fashioned from the State Model Court Security Plan.

Currently, the state has 100% compliance by all courts in completion of a local security plan. This accomplishment took the full support of the AOC and direct communication with the AOC Office of Court Security and local courts. When the AOC began its initiative to push the completion of a Model Court Security Plan, some counties initially chose not to comply. To enforce its authority requiring completion, the AOC had to try a case in a court of law. The legal action, while undertaken reluctantly, set the tone for other counties to know that the AOC was serious about enforcing compliance.

It is important to note that compliance in completing a local security plan does not require that a court meet all of the standards included in the Model Court Security Plan. Instead, the local security plan serves as a tool for courts to address their security issues in a comprehensive manner. Currently the AOC is pursuing legislation to provide court security funding through surcharges on filings to generate approximately \$20 million per year. These funds would be used to support grants to help offset the costs of implementing the State Model Court Security Plan. Unfortunately, the legislation has stalled with the recent economic downturn although the AOC has hopes that it will gain traction again in the future.

Funding is the single largest obstacle to implementing the Model Court Security Plan in all courts. There are not enough funds for all courts to meet the model plan; however, the state has made significant strides in recent years on key elements such as weapons screening, officers in the courtroom, and prisoner transportation. For example, the assessments completed in the last several years identified a number of municipal courts which had no weapons screening. Once this was identified, the AOC required these courts to address this problem.

Enforcement of security standards is a constant battle for the State Office of Court Security. With recent budget cuts, courts are asking the AOC if they could discontinue various security protocols. Fortunately, the local courts won't make changes without AOC permission and the State Security Office has been able to continue to enforce basic security protocols.

Ohio

Ohio is unique from the other state courts examined because it is the only non-unified court system out of the five that has home rule. The Supreme Court Rules of Superintendence established a set of Court Security Standards and required that courts complete a security plan. Although the state requires local courts to complete security plans, since Ohio has home rule, compliance enforcement is not possible.

The Ohio Supreme Court maintains an Office of State Court Security which serves as a resource to the state's courts for improving local security programs based on the Supreme Court Rules of Superintendence and State Court Security Standards (see appendices). The resources offered include completing risk assessments, facility planning and design help, security and emergency planning help, security personnel training, COOP training, and staff personal safety training. Although many courts reportedly work with and use the services of the Security Office to improve security programs in their courts, the office does not keep a database of which courts are meeting the state's security standards.

The Rules of Superintendence and Security Standards were created through a large 50 person Advisory Committee on Court Security and Emergency Preparedness with representatives from all of the major justice system stakeholders including judges, police, prosecuting and defense attorneys, sheriffs, and county government. As a non-unified court system the Office of Security does not keep track of local court security compliance to state standards or how many courts have a security plan in place; however, the office is under the impression that many of the state's courts prefer to take advantage of the offices resources on a voluntary basis and would be more reluctant to do so if compliance were more strictly mandated.

Oregon

Oregon is a unified court system which includes 36 circuit courts, three appellate courts and over 100 municipal and justice courts. The AOC maintains an Office of Court Security

which is overseen by the state Director of Security. The Director is tasked from the Chief Justice to oversee and support the various security programs and initiatives currently underway in the state. The implementation of a statewide court security plan in Oregon has gained considerable traction in the last six years. The State Security and Preparedness Committee (SSPC) was established by Chief Justice Order in May 2004 and was charged to:

- Review and make recommendations on the development, revision, and utilization of local security, emergency preparedness, and response plans.
- Identify and draft legislation concerning security, safety, and emergency preparedness.
- Develop training opportunities in security, safety, and emergency preparedness for Oregon Judicial Department staff.

From the State Security Committee a number of statewide security initiatives were put into action. These included state statutes requiring local court security advisory committees, security plans, and a state model court security plan. Following the advisory committee recommendations, the Oregon Judiciary in 2008 initiated a five year state court security implementation plan to ensure that all court facilities statewide meet a set of minimum standards for maintaining court security.

All judicial districts in Oregon are required by state statute to convene a Court Security Advisory Committee with representatives from the courts (preferably the presiding judge of the circuit court), law enforcement and county government. The advisory committee is required by statute to prepare local court security plans, emergency response plans, and COOP plans for every court facility in their jurisdiction.

Oregon has a model court security plan to use as a template for developing local security plans (see appendices). The model court security plan was developed in 2005 by the AOC with the guidance of the SSPC. The State Director of Security oversees development of each judicial district security plan and reviews each plan for completeness.

Although the county sheriff of each judicial district is responsible for providing court security in Oregon, the State Judiciary has a court security funding account which the Director of Security oversees to fund security physical infrastructure improvements (e.g., weapons screening

equipment, surveillance equipment, duress alarms, etc.). Allocation of these resources is partly based on security assessments completed as part of the local security plans collected by the Judiciary.

Oregon has full compliance in terms of having security plans in place for all of its judicial districts. It may be hypothesized that the availability of a state security funding account and statutory requirements put in place by the state legislature help to ensure that judicial districts submit their security plans as required by the Judiciary.

Utah

Utah has a unified court system with a strong centralized management structure as compared to many state court systems around the country. The chief justice and Judicial Council have backed and given full authority to the State Security Director for overseeing security programs statewide and serving as a resource for local courts in developing security plans. All Courts of Record in the state of Utah² are required by the Judicial Council's Court Rules to have a written security plan on file with the Administrative Office of the Courts and updated on an annual basis.

Utah did not have a State Court Security Director until 2007 and prior security programs were relatively limited in their scope. In the past, only emergency management plans were required to be submitted (i.e., fire, shootings, etc.) by filling out a small pamphlet. Today, security plans are required to include such items as procedures for weapons screening, high profile trials, prisoner transport, bailiff responsibilities, and court employee responsibilities. In recent years local court security plans have been expanded; however, the content of the security plans is not necessarily consistent among the courts. The Director of Security readily admits that the content of many local security plans is generally not up to the AOC's standard. The intent of expanding the security plans to include law enforcement responsibilities is to initiate conversation between local court executives and county sheriffs based on the premise that communication and agreement on court security between the courts and county government is critical to the safety and security of court employees and visitors to the court.

² There are 35 Courts of Record in the State of Utah.

Utah does not have a statewide model court security plan. In lieu of a model court security plan, a plan template is typically used based on the Salt Lake City Courthouse Security Plan. The template can be revised by other courts as is reasonable for their own needs. For example, the Salt Lake City Plan includes a section on camera security which does not apply to a number of smaller rural courthouses. For each individual court there is a certain amount of discretion for making local decisions about what the plan should and should not include.

Utah admittedly does not have a comprehensive security program requirement for its state courts. For example, there are no state requirements establishing local court security committees and no security assessments as part of local security plans (although it is recommended and the AOC offers assistance for completing these). It should be noted, however, that Utah is currently initiating a statewide security audit which began in November 2010. The assessment will include operations and facility review of all courthouses in the state. This will be the first statewide security audit conducted in Utah and will provide valuable information on compliance with procedures and facilities standards.

The state does has full compliance in that all Courts of Records currently have a local security plan on file with the AOC.³ The success Utah has had in getting compliance can be credited to the fact the Director of Court Security offers a significant amount of support in developing the plans and the Judicial Council in Utah wields strong authority over the individual Courts of Record. Completion of local security plans is a collaborative process between the local courts and the Director of Court Security. The Director of Court Security reviews, analyses and makes suggestions for each individual court security plan. Local court executives appreciate the assistance provided because they are often not familiar with the subject matter and may have difficulty completing the assessments on their own. In the final analysis it appears that the hands-on approach the Director of Court Security has taken is making a significant impact as opposed to unsupported directives from the Judicial Council.

³ Note: Utah has security plans in place for all of its Courts of Record, but not for its Justice Courts (limited jurisdiction).

III. Review of Security Plan Subject Area Requirements

The specific components that should, if applicable, be included in an individual court security plan include both general security elements and operational security elements (see table 4-1 below for a complete list of court security plan subject areas). In a review of five states' court rules requiring courts to have security plans in place, it was discovered that specific subject areas were not detailed in the statutory or court rules. In fact, only California's Rule of Court details the complete list of plan elements included in table 4-1 below.

Although the other states reviewed do not list specific security plan subject areas which are required to be addressed in their statutes or court rules, this is not to say that they do not have other mechanisms in place for addressing these topics. In both Oregon and New Jersey, for example, the AOC has put in place model court security plans which all local court security plans are to be tailored after. These model security plans are akin to a set of best practices which local courts are encouraged to incorporate when developing their security plans. In interviews with court officials from the two aforementioned states, it was stressed that there is no 'one-size fits all' security plan for all courts and that officials have made attempts to prioritize critical elements. In measuring compliance, the court security officials from New Jersey and Oregon emphasized that they do not require that courts address all the issues in the model plan, but do require that courts are at least aware of the issues and are taking steps to address at least the most critical ones identified. As measured through this viewpoint, both Oregon and New Jersey have achieved 100% compliance in receiving security plans from all of its courts.

Table 4-1: Court Security Plan Subject Areas	
General Security Subject Areas	Security Operations Subject Areas
Mail handling security	Security personnel and staffing
Identification cards and access control	Perimeter and entry screening
Courthouse landscaping security plan	Prisoner and inmate transport
Parking plan security	Holding cells
Interior and exterior lighting plan security	Interior and public waiting area security
Intrusion and panic alarm systems	Courtroom security
Fire detection and equipment	Jury trial procedures
Emergency and auxiliary power	High-profile and high-risk trial security
Use of private security contractors	Judicial protection
Use of court attendants and employees	Incident reporting and recording
Administrative/clerk's office security	Security personnel training
Jury personnel and jury room security	Security staff training
Security for public demonstrations	Courthouse security communication
Records storage security	Hostage, escape, lockdown, and active shooter procedures
Evacuation planning	Bomb threats
Security for after-hours operations	Firearms policies and procedures
Custodial services	Restraint of defendants
Computer and data security	
Workplace violence prevention	
Public access to court proceedings	

In Arkansas, the state AOC does not have a model security plan in place but has put together a security plan outline which includes a complete list of plan elements for local courts to include. Although the state does not have full compliance in all topic areas (or even in getting security plans for some courts), the outline serves to guide plan development and the completeness of the security plans received has greatly improved since the security plan requirement was made in 2007.

In Utah there is no model security plan in place; instead, local courts are expected to model their plans after the Salt Lake City Courthouse Security Plan which is generally considered the most comprehensive in the state. Using the Salt Lake City template and with the hands-on assistance of the State Security Director, all Courts of Record in Utah have a local Court Security Plan in place. It should be noted, however, that the state is currently in the process of completing a statewide security assessment of all of its Justice Courts and it is

expected that substantial modifications in many local court security plans will be made once the results of the assessments become available.

The state of Ohio differs from the other courts reviewed in that it is not a unified court system and the AOC has neither the authority nor the desire to enforce security plan completeness. Although the Supreme Court has issued a directive that all courts shall have a security plan in place, there is no language specifying the components that the security plan shall address. That being said, the AOC has put together a set of Court Security Standards (see appendices) as a resource for courts to reference specific security component elements and implement as suited for local purposes.

IV. Recommendations for California Rule of Court 10.172 and for Improving Security Plan Compliance in Local Courts

Compared to some of the other unified court systems reviewed, California has only recently implemented its requirement for court security planning and initially has struggled with getting compliance from all of its courts. However, it is clear that compliance has been increasing since California's Court Rule 10.172 was adopted in January of 2009. This is clearly evidenced through the following compliance information provided to the NCSC:^{4, 5}

- The initial deadline for all of the state's courts to complete their security plans was November 2009.
- As of March 2010, only 14 of 58 (24%) courts had completed one.
- As of April 2010, 24 of 58 (41%) courts had submitted their security plans.
- As of August 2010, 39 of the 58 (67%) courts had submitted plans; of these, 30 were considered complete and in compliance with the requirement of Court Rule 10.172.
- As of July 2011, 49 of 58 courts (84%) had submitted plans, all of which were deemed complete or in the process of being revised for completeness so as to be in compliance with the court rule.

⁴ Compliance information as of August 2010 and July 2011 was referenced from: "Annual Report Summarizing Court Security Plans Reviewed by the Judicial Council Report to the Legislature." Judicial Council of California, July 2011. Earlier compliance information as of March and April 2010 was provided to NCSC staff via email correspondence with senior AOC officials.

⁵ The NCSC does not have data on the number of plans submitted in this time period which were considered complete vs. the number considered incomplete. In making determinations about compliance, plans addressing all of the required court rule subject matter areas are deemed complete while failure to address all of the required areas results in a finding that the plan is incomplete or deficient.

The data above indicates that California courts have made significant progress in developing their court security plans. This being said, there is still room for improvement and there may be some lessons learned through the experiences of other states that have gone through similar efforts to implement court security planning in their courts. Interviews and data collected from multiple states included in this report shed some light on a number of initiatives that have helped state court systems improve security planning in local courts.⁶ Based on other states experiences, it is recommended that California consider the following strategies as it investigates additional ways for improving its Rule of Court and strategies for improving security plan compliance:

1. Continue to promote the online security plan template and completion tool.

To increase compliance and to make it easier for local courts to complete their security plans, the California Judicial Council has developed an online security plan template and completion tool. This online tool has similar content to what can be found in the security plan outlines published by the state of Arkansas AOC, but is much more sophisticated to the extent that it is an interactive vehicle for individual courts and AOC officials to use collaboratively in developing standardized court security plans for the entire state. Although the state does not currently have full compliance in getting security plans from all local courts as noted above, the online resource serves as an intuitive and thorough guide for assisting local courts and seems to have had a very positive impact. In fact, since the online templates and tools were deployed in February of 2010, the number of courts who have completed their security plans has increased dramatically (refer to compliance information presented on preceding page).

A positive impression of the online tools was shared in interviews with state court security officials⁷ who expressed that the existence of the online security planning template and tools has significantly benefited the AOC's ability to manage and collaborate with individual courts in completing their plans. The positive feedback and recent increases in compliance are encouraging and may indicate that the online security plan template and tools are reaping tangible benefits. As more and more courts become comfortable with the online tool and

⁶ Although California differs from many other states in terms of size, funding and organizational structure there are still opportunities to learn from other states experiences as related to implementation and compliance in court security planning.

⁷ NCSC project staff interviewed a Regional Court Security Coordinator and Security Analyst for the state Office of Emergency Response and Security in completing its review on the state's online template and tools.

educated on the topics included within the template, it is inevitable that the overall courts community in California will become more educated on the importance of court security planning. Ideally, courts that have completed their plans will positively influence other courts into coming into compliance as well through peer influence.

2. Enhance and augment the online model security plan content to provide local courts more resources when completing online security plans.

The NCSC believes that the online tool has had a very positive influence on implementation of Court Rule 10.172; however, there may be potential to further enhance and upgrade the online tool. For instance, the number of topics covered and amount of technical detail required to complete the security plan per the requirements set forth in California Court Rule 10.172 is considerable and the online security templates may be intimidating to some court executives not experienced in developing security plans and thus may be negatively affecting compliance. In many courts in California, as is the case in many places throughout the country, there are no staff specifically trained or dedicated for the development and coordination of local court security plans; therefore, completing the online security plan is often a daunting task. Because of this reality, it may be desirable to add supplementary information to the online tool including background information and best practices of court security⁸ in order to introduce and educate users of the online security plan template about required court security topic areas which they may not otherwise have experience with. This could be done simply by adding information to the online template topic areas and would conceivably not involve significant alterations to the online tool.

3. Increase AOC Security Coordinator Manpower to Assist in Local Court Security Plan Development.

The online tool initiated by the California Judicial Council is a tremendous means for supporting local courts in completing their security plans; however, given the time and technical expertise involved in completing the security plans the AOC, based on funding, may want to consider assigning additional staff to provide more direct oversight, support and encouragement

⁸ The NCSC publication, “*Steps to Best Practices for Court Building Security*,” published in February 2010 may be a good reference. The document is publicly available online at:
<http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=155>

of local security plan development. Currently, the California AOC maintains four regional Emergency Response and Security field offices with each office staffed by a security coordinator. The coordinators are charged with working with local courts to obtain compliance with the Rule of Court and reviewing all security plans submitted.

One of the security coordinators' roles is to assist local courts in completing their security plans; however, because of the large number of courts that each coordinator is assigned to assist and because of their other responsibilities, there is simply not enough manpower available for the AOC to offer direct hands-on assistance to local courts in completing their security plans. Instead, the coordinators must rely on the online templates and encourage local courts to use other local courts as a resource. For example, a court may communicate with other courts of similar size and/or composition that may have already completed a security plan and, if amenable, may be able to use already completed security plans as a reference for completing their own.

Although it is difficult to quantify the impact of having additional AOC staff on the ground working directly in the local courts, interviews with other states indicate that local compliance is directly influenced by direct AOC staff involvement in the security planning process. This involvement should take the form of in-person participation in court security planning meetings and continual checking-in with local judges and court executives to monitor plan development.

4. Create Security Improvement Grant Fund.

In Arkansas, like in California, there are court rules that establish the requirement that trial courts complete security plans. However, in Arkansas the administration of a security project grant fund creates a much greater incentive for local courts to develop a security plan than the court rule directive alone; in order for courts to be eligible for grant funding, they must first develop a court security plan. California should consider the creation of a similar grant fund for courts to make security improvements with eligibility at least partially dependent on the completion of a security plan.

5. Initiate Stricter Enforcement of Existing Court Orders.

From interviews with all of the State Court Security Directors included in this review, it is clear that the improvement of court security and the accompanying buy-in and participation from local courts cannot occur unless directives are made with appropriate authority and unless those persons in authority are willing to wield that authority in an effective manner. To get better compliance the California Judicial Council/AOC may want to take a harder line in enforcing Court Rule 10.172.

New Jersey is an example of a state whose AOC chose to enforce its court security plan through legal action. In one instance where a particular county was non-compliant with addressing the law regarding court security planning, the AOC brought the case to a court of law and the resulting decision in favor of the AOC set the tone for other county courts in New Jersey to comply with the court rules. While legal action is an extreme example and is not recommended unless no other alternatives are present, it does demonstrate the importance placed on court security planning by the New Jersey AOC and the resulting compliance.



Superior Court of California County of Orange

CHAMBERS OF
FREDERICK P. HORN
JUDGE

700 CIVIC CENTER DRIVE WEST
P.O. BOX 1994
SANTA ANA, CA 92702-1994
PHONE: (657) 622-5231

June 5, 2012

Hon. Douglas P. Miller
Associate Justice of the Court of Appeal,
Fourth Appellate District, Division Two
3389 Twelfth Street
Riverside, California 92501

Re: Final Report of the Court Emergency Response and Security Task Force

Dear Justice Miller:

Thank you for taking the time to speak with me regarding the recent release of the report of the Strategic Evaluation Committee (SEC) and how it relates to the work of the Court Emergency Response and Security Task Force, which I chair. The task force and I wanted to share with you, at the earliest moment, some background about the task force and the work that the task force has conducted over the past five years. Our intent is to provide you with preliminary information that may assist you and the Executive and Planning Committee as you determine the process for the Judicial Council's consideration of the SEC's report and recommendations regarding court security. We look forward to meeting with you later this month to discuss these important issues, and would also like to offer to you, the Executive and Planning Committee, and the Judicial Council any assistance the task force can provide relative to determining how court security should be implemented in the judicial branch.

Background

On August 15, 2007, Chief Justice Ronald M. George (Ret.) established the Judicial Council's Court Emergency Response and Security Task Force, appointing me as its chair. In forming the task force, the Chief Justice brought together representatives from existing statewide advisory groups that had been formed to address security and emergency planning in the trial and appellate courts.

The charge of the task force requires it to:

- Evaluate emergency planning, continuity of operations, court security, and personal security issues and develop recommendations for the Judicial Council to manage, maintain, and improve security in

Attachment B

Page 2

the courts through statewide systems and progressive initiatives to increase efficiency, effectiveness, and cost-saving measures in California;

- Provide an interim report to the Judicial Council after 18 months; and
- Provide a final report of recommendations to the Judicial Council at the end of its term.

The task force was originally scheduled to complete its work and report to the Judicial Council by August 2010; that deadline was extended first to December 2011 and then to June 2012. These extensions were due to the significant changes in the funding of court security due to the intervening realignment legislation. In light of our conversation today, the task force will delay finalizing the report, so that it can work with you and the Judicial Council to determine the best approach to completing a report that best addresses the crucial security needs of the branch.

For the past five years, the task force has been working on recommendations to improve security in California. Examples of recommendations include:

1. Determining how best to provide comprehensive court security to judges, courts, staff, and the public we serve;
2. The preparation and review of (1) court security plans, (2) emergency plans, and (3) continuity of operations plans;
3. Providing education to judges and court staff concerning personal and court security;
4. Developing a branchwide threat and incident program;
5. Reviewing and evaluating branchwide staffing and service standards; and
6. Establishing a standing Court Security Advisory Committee to provide oversight on these efforts and continue to review and evaluate court security and advise the Judicial Council.

The SEC Report

The task force has reviewed the recommendations of the SEC. The task force agrees with the SEC overarching recommendations of limiting the AOC's functions to the charge of the organization, eliminating redundancies, and performing services with the greatest amount of efficiency and transparency. However, the task force preliminarily takes issue with several of the specific SEC security-related recommendations described below.

Recommendation No. 7-54: The SEC suggests that there is no need for a stand-alone Office of Emergency Response and Security (OERS). The task force respectfully disagrees. Most of the functions of the current OERS require specialized training and experience that cannot be performed effectively by administrative staff personnel untrained in judicial security and law enforcement

Page 3

techniques. Physical security recommendations, building design, threat assessments, and privacy protection techniques should appropriately remain the responsibility of OERS.

Unlike virtually any other institution in our society, the judicial branch has the authority to compel citizens to attend court, involuntarily, as jurors, witnesses, or parties in connection with civil, family, criminal, dependency, or other cases that are pending. The task force submits that with this authority comes a moral responsibility to provide a civilized environment uncorrupted by threats and avoidable risks to those who enter the courthouse. In the view of the task force, a stand-alone OERS appropriately placed within the organizational structure is crucial to optimizing the delivery of a secure environment.

Recommendation No. 7-55: The SEC suggests that the functions of the OERS should be refocused and limited to those reasonably required by statute or by rules of court. At this time, without addressing the suggestion to limit the functions of OERS, the task force respectfully agrees that OERS should continue the most important core functions of assisting in the preparation and review of court security plans for new and existing facilities; emergency plans; and continuity of operations plans; as well as providing support concerning court security equipment, if requested by the courts.

Recommendation No. 7-56: The SEC recommends elimination of online protection functions. The task force respectfully disagrees.

In the highly specialized world of dignitary protection and threat assessment, experts agree that privacy protection, namely the ability to “hide in plain sight,” is the first line of defense for judicial officers. Judicial threat assessment studies undertaken by the U.S. Marshals Service and others make it clear that judges are most vulnerable away from the courthouses where their security provider is located. Once a judge leaves the building, he or she is not normally assigned a protective detail.

To put this in historical context, in the last century, 34 judges were killed by non-family members, 13 were killed at the courthouse (most of which were killed before weapon screening procedures were instituted), another 21 were killed away from the courthouse. Of the judges killed away from the courthouse 10 were killed in transit and 11 were killed at home. In addition, 4 spouses were also killed. It is beyond dispute that judges are most vulnerable at home.

Protecting home address information has become critical to improving a judge’s safety. The California Legislature has specifically recognized that danger and provided California Public Safety Officials with home address privacy protection tools not generally available to other members of the public. (See Gov. Code sections 6254.21 and 6254.24; Elections Code section 2166.7; Vehicle Code sections 1808.2, 1808.4, and 1808.6)).

One of the collateral impacts of an effective entry weapons screening program is that it forces potential stalkers and attackers to focus their efforts to attack judges away from the courthouse. In the Internet age, obtaining home address information online can be very easy IF the judge does not take early affirmative steps to block or mask that information.

Page 4

Many of the solved cases in the last several decades wherein suspects have stalked, harassed, or killed a judge involve pre-planning and research on the part of the suspect, primarily through Internet searches and public records checks and NOT by physically following the target, which would expose the stalker to potential detection.

The SEC report suggests that the OERS online security function may be better left to local courts or to judicial officers themselves, citing a recent California Judges Association arrangement with a private vendor to submit opt-out demands of Internet data vendors for an annual fee. The task force respectfully disagrees with the SEC's suggestion because leaving the responsibility to the individual judges will likely mean it will not be done by judges who do not have the skill set to do it. It is also counter-productive to pull judges away from their judicial functions in order for them to sit at their keyboards and try to figure this out individually.

Moreover, the release of an outsourced list of home addresses and telephone numbers of all of our judicial officers should never be entrusted to a private vendor who has not undergone a law enforcement background check. The loss of this information could be disastrous to the judicial branch.

In addition, the expense of hiring an outside vendor to perform the Internet opt-out demand (See Gov. Code section 6254.21 (c), et seq.) would be far more expensive. The current cost for most private online privacy protection services is more than \$100 per person. There are 2,044 judicial officers and approximately 3,400 additional family members currently served by the OERS Judicial Internet Opt-out Program. The expense in outsourcing this task would be much more costly than doing it in house.

Having one trusted, background-checked OERS employee handling all statewide judicial opt-out demands is much more effective and cost-efficient than training 58 local court administrative staff members or 2,000+ judicial officers to perform the same task.

Lastly, OERS uses the updated current national list of Internet data vendors published by the California Office of Privacy Protection (COPP). Many of the private online protection services do not make opt-out demands of the major Internet data vendors on the COPP list. A judge using a private online opt-out service which does not cover all of the major Internet data vendors would be given a false sense of security and still be exposed.

The task force strongly recommends that the OERS judicial Internet opt-out program remain intact.

Finally, the task force also recommends that if the Judicial Council chooses to follow or implement the SEC recommendations relating to court security functions, that it allow the task force or the proposed Court Security Advisory Committee to provide input regarding future judicial branch security-related issues.

June 5, 2012

Page 5

We look forward to meeting with you later this month at your convenience.

Sincerely,

A handwritten signature in black ink, appearing to read "F. P. Horn", written in a cursive style.

Hon. Frederick Paul Horn, Judge
Superior Court of California, County of Orange

FPH/lg

By e-mail

cc: Jody Patel, Interim Administrative Director of the Courts
Curt Soderlund, Interim Chief Deputy Director



Judicial Council of California · Administrative Office of the Courts

455 Golden Gate Avenue · San Francisco, California 94102-3688

www.courts.ca.gov

REPORT TO THE JUDICIAL COUNCIL

For business meeting on: December 13, 2011

Title	Agenda Item Type
Judicial Branch Administration: Report from the Judicial Council's Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch (No Action Required)	Information Only
	Date of Report
	November 4, 2011
Submitted by	Contact
The Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch	Althea Lowe-Thomas, 415-865-4987
Hon. Richard D. Huffman, Chair	althea.lowe-thomas@jud.ca.gov

Executive Summary

This is an informational report by the Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch (A & E Committee) on their preliminary review of the core functions, funding levels and sources, and staffing of Administrative Office of the Courts (AOC) divisions; and identification of collaborative efforts among divisions.

Previous Council Action

At the August 26, 2011 business meeting, the Judicial Council requested the A & E Committee begin a structural and fiscal review of the AOC divisions and report back to the council at its next educational meeting on key findings to date.

Methodology and Process

The A & E Committee was created in June 2010 by former Chief Justice Ronald M. George in order to promote transparency, accountability, efficiency, and understanding of the AOC and the judicial branch. The advisory committee fosters the best use of the work, information, and recommendations provided by the AOC, and it promotes increased understanding of the AOC's

mission, responsibilities, accomplishments, and challenges. The A & E Committee is charged with reviewing and recommending on budget change proposals for the AOC, changes in the annual compensation plan for the AOC, financial audit reports for judicial branch entities, making recommendations on any practices that will promote efficiency or improve financial accountability in the Judicial Branch, and advising on other issues related to the committee charge as requested by the Chief Justice, Judicial Council, or the Administrative Director of the Courts.

The AOC consists of 13 divisions and the Executive Office which currently has two major units, Office of Communications and Office of Emergency Response and Security. The A & E Committee met on September 1 and 2, 2011 and received presentations from the AOC division directors (or their representatives) about AOC division organizational structure, core functions, services provided, and fiscal and position summaries. An overview of the Executive Office was presented during a follow-up conference call on October 7, 2011.

The committee formed an Education Subcommittee to further study each AOC division's five-year budget summaries by funding source and program/project, and staffing levels by division, including full time employees, and temporaries. The Education Subcommittee met three times by telephone and has reviewed and discussed the following materials which are included as Attachments 1 through 16 to this report:

- AOC Historical Human Resources Metrics Summary (2006-2011) – includes information by division or unit on authorized positions, vacancy rates, full time employees, and 909¹ and agency temporaries.
- Division overview materials, organizational charts, and five year fiscal summaries by division or unit (fiscal years 2006-2007 to 2010-2011).

Education Subcommittee members also conducted brief follow-up interviews with AOC Directors prior to the council meeting.

Attachments

1. AOC Historical Human Resources Metrics Summary (2006-2011)
2. Combined Five-Year Fiscal Summary of all AOC Divisions
3. Executive Office
4. Office of Communications (OC)
5. Office of Emergency Response and Security (OERS)
6. Regional Office

¹ The 909 category is the State Controller code the AOC uses to reference a temporary position or a temporary employee. These positions are not generally funded through the Budget Act and are categorized as temporary positions used in the absence of an authorized position. This may include retired annuitants and grant funded employees.

7. Center for Families, Children, and the Courts (CFCC)
8. Court Case Management System Program Management Office (CCMS-PMO)
9. Court Programs and Services (CPAS)
10. Education Division/Center for Judicial Education and Research (EDUC)
11. Finance Division (FIN)
12. Human Resources Division (HR)
13. Information Services Division (IS)
14. Office of Court Construction and Management (OCCM)
15. Office of the General Counsel (OGC)
16. Office of Governmental Affairs (OGA)
17. Trial Court Administrative Services Division (TCAS)

Office of Emergency Response and Security

Malcolm Franklin
Senior Manager

Overview of Administrative Office of the Courts Programs and Resources Office of Emergency Response and Security (OERS)

I. Organizational Structure of the Division and Services Provided

General Description of Structure and Services

1. The OERS was created in 2005 and is a small unit within the AOC Executive Office division. It currently has 9 employees (and one agency temp secretary). Because it is small, OERS is not divided into subgroups. Staff responsibilities overlap and are shifted as needed, to ensure the team is working together to handle its highest-priority work.
2. The OERS spearheads work on the Judicial Council's goal to ensure the safety and security of the courts and ensure continuity of operations planning (Goal III, Objective 3) and provides security expertise in support of the council's goal for facilities and technology infrastructure (Goal VI, Part A Objective 2 and Part B Objectives 3, 4, and 7).
3. The OERS provides specialist advice, expertise, programs, and services to the superior and appellate courts and to the Judicial Council, upon request, in three areas: Physical Security, Personal Security, and Emergency Planning. It also works on additional initiatives that provide significant out-of-sight services to support the courts, council, and AOC.
4. The majority of requests for OERS advice and assistance are from the superior (trial) courts. OERS administers programs to provide equipment and enhancements exclusively to the trial courts. OERS uses regional security coordinator assignments as the most effective way to address requests that usually require travel to and assessment of trial court facilities.
5. With the exception of entrance security screening equipment and critical security enhancements for the trial courts, OERS pays for program and service expenses through its general fund allocation. This covers costs related to court-requested consultations, trainings, badge supplies, emergency equipment, council advisory groups, and resources.

Additional Details of Programs and Services

Physical Security

The most essential core function of the unit is its physical security programs and services, as OERS provides assessments that the trial courts cannot easily get elsewhere and pays for critical court security enhancements and equipment. As an example:

- "On the ground" assessments and assistance to courts, including help with presentations.
- Court security plan guidance, templates, and tools to help trial courts meet requirements.
- Consultation on security related aspects of facility modification and construction projects.
- Program that pays for entrance security screening equipment replacement for trial courts.
- Program that pays for critical security enhancements and maintenance for trial courts.
- Management of statewide master agreements to save courts money on quality equipment.
- Subject matter expertise in the form of advice, publications, guides, best practices, etc.

Personal Security

The next most essential function is its personal security programs and services, as OERS advises judicial officers who are under threat and aids them in removing their home address and phone from major online data vendor websites. As an example:

- Remote and in-person consultation/evaluation for judicial officers who are under threat.
- Coordination of communication about threats and incidents with law enforcement.
- Program that helps judicial officers with online privacy protection (as noted above).
- Subject matter expertise in the form of advice, publications, guides, trainings, etc.

Emergency Planning

Following that is its emergency planning programs and services, as OERS provides a dedicated emergency planner, tools, training, and ongoing assistance to trial and appellate courts for continuity of operations. As an example:

- On call advice and support for court emergency planning, management, and response.
- Emergency and continuity of operations plan guidance, templates, and tools for courts.
- Program that pays for/provides training of court emergency planners on web-based tool.
- Management of statewide master agreements to save courts money on quality equipment.
- Subject matter expertise in the form of advice, publications, guides, trainings, etc.

Additional Initiatives

OERS also does significant work in addition to its high-profile programs and services for courts. As an example:

- Program that background checks AOC contractors and helps court subscribers to CLETS.
- Program for badges and access that enhances security in AOC offices for staff/visitors.
- Program for emergency response team to aid in safe evacuation of AOC staff/visitors.
- Program for emergency equipment to help meet legal requirements for a safe workplace.
- Subject matter expertise to advisory groups and work on reports to the Judicial Council.

II. Division Accomplishments/Achievements since Fiscal Year 2005–2006

General Description of Accomplishments

1. OERS began from scratch, evaluating 58 trial courts with over 450 facilities to assess requirements, centralization, and standardization in branch emergency and security matters. Based on needs identified by the council and courts, OERS created or took on programs and services that support the council's goal on safety and security in the courts.
2. OERS developed and maintained a web-based planning tool, free-of-charge to the courts, to simplify setup procedures, standardize formats, and create a single data repository—in addition to other work that supports council goal on technology infrastructure.
3. OERS provided subject matter expertise and created and implemented many contracts, tools, trainings, and educational materials for physical security, personal security, and emergency planning—work that supports the two council goals mentioned above as well as the council goal on facilities infrastructure. Additional details follow for each area.

Additional Details of Accomplishments

Physical Security

OERS has been asked for assistance by all 58 of the trial courts and 1 of the appellate courts, advising on issues ranging from general best practices to specific active shooter procedures and in one case, providing peace officer assistance at a high-profile trial at the request of a court. Work samples follow.

- *Court Security Assessments*—Provided approximately 400 total on-site facility security assessments at the trial courts’ requests, reporting observations and recommendations to the presiding judges and court executive officers on the areas of perimeter security, interior security, electronic security systems, and more.
- *Court Security Plan Assistance*—Developed and maintained guidance and a module for the OERS web-based planning tool to automate court security plan creation and help the trial courts comply with legislatively-mandated requirements, offered staff assistance to the courts, evaluated submissions for the AOC, and wrote annual reports for the council.
- *Courthouse Improvement Consultation*—Provided security expertise on court facility modification/construction projects from the Judicial Branch Five-Year Infrastructure Plan and its Trial Court Capital-Outlay Plan, assessing/reporting on security-related aspects of planning, design, construction, facility management, and risk management on projects such as the B.F Sisk Courthouse in Fresno and the Plumas/Sierra regional courthouse.
- *Screening Equipment*—Ran the Entrance Screening Equipment Replacement Program to help all trial courts get screening equipment and replace outdated/broken equipment, tracking and evaluating hundreds of pieces of screening equipment in the trial courts and purchasing over 650 x-ray and/or magnetometer units and over 230 extended service agreements for the courts to date using ongoing funds from the governor’s budget, which saved the courts hundreds of thousands of dollars in FY 2010–2011 alone.
- *Security Enhancement*—Administered the Trial Court Security Grant Program to help the trial courts with critical security enhancements to systems and equipment, purchasing and overseeing the installation/maintenance of over 130 duress alarm projects and over 100 access control and/or video surveillance projects, including work on integrated security systems for a pioneering “Future Courts Project” in Santa Cruz, using an allocation from a special fund that is restricted to trial court improvements.
- *Statewide Contracts*—Facilitated court access to high-quality, reasonably-priced security equipment that is vetted by specialists by managing statewide master agreements.
- *Subject Matter Expertise*— Created physical security related publications and templates, including self-assessment and best practices documents as well as innovative Radiation Protection Program guidance for courts to simplify complex registration, documentation, and training requirements for x-ray machines.

Personal Security

OERS has been asked for assistance by judicial officers in all 58 of the trial courts and all 7 of the appellate courts, advising judicial officers who are under threat and aiding them in removing their home address and telephone number information from major online data vendor websites. Work samples follow.

- *Consultation and Evaluation*—Provided dozens of remote and in-person consultations to judicial officers whose personal security was threatened, offering advice and assistance in evaluating incidents and collaborating with OERS team members to obtain assistance with security enhancements or get help with online privacy protection.
- *Threat/Incident Coordination*—Assisted with coordinating and creating a clear path of communication between the many agencies and jurisdictions involved in threats against judges (which are required to be reported to CHP), and with incidents in the courthouses that are a security concern but not currently required to be reported by law.
- *Internet Privacy Protection*—Provided and maintained guidance and services such as the Judicial Privacy Protection Opt Out Program, which has assisted over 2,000 California judicial officers and their families with privacy rights granted to them by law by having their home address and telephone number information removed from up to 15 major online data vendor websites that sell or share information with others.
- *Information and Strategies*—Developed and maintained publications, including inclusive Privacy Protection Guidance about online privacy issues and strategy, and created and provided trainings and broadcasts for court information and education, including training and presentation of programs and services at New Judge Orientations.

Emergency Planning

OERS has provided the trial and appellate courts with a dedicated emergency planner, tools, trainings, and ongoing assistance to aid them in emergency and continuity planning efforts. Work samples follow.

- *Guidance and Support*—Provided advice and support to the courts for emergency response issues and questions ranging from bomb threats to shelter in place practices and assisting with emergency management, sharing personal information received from facility managers and law enforcement. As AOC headquarters is housed in the same facility as the Supreme Court and Court of Appeal, First Appellate District, OERS also shares advice and support at tenant meetings with the courts and building management.
- *Planning Assistance*—Provided advice and expertise to the superior and appellate courts on request, and assisted them with the creation of emergency plans used to respond to any incident prior to the activation of a Continuity of Operations Plan (COOP), of COOP used to identify a chain of command and resources to continue critical operations and recover in an extended emergency situation, and of command and control plans that focus on emergency operations centers, instructions for senior leadership, and communications.

- *Training and Tools*—Developed and maintained a web-based planning tool for the courts to help ensure that mission critical functions continue in the event of a disaster, and administered the Continuity of Operations Planning Program to train court executives and court emergency planners upon request (to date, training on the web-based planning tool was provided to over 90 percent of the courts upon request, facilitating development of over 400 plans and providing ongoing assistance and evaluation to the courts).
- *Statewide Contracts*—Facilitated court access to high-quality, reasonably-priced emergency notification systems by managing a statewide master agreements.
- *Subject Matter Expertise*—Made expertise easily available to the courts by preparing and providing emergency planning publications, templates, tools, training, and other educational materials.

Additional Initiatives

OERS supplied other programs and services in addition to the high-profile work done for courts. Work samples follow.

- *Background Checks*—Helped trial court and branch subscribers to the California Law Enforcement Telecommunication System (CLETS) comply with Department of Justice requirements through the CLETS-Related Background Check Program by processing over 2,100 background check requests from AOC contacts for AOC contractors and by monitoring and maintaining badges for over 800 active contractors who currently supply services related to court facilities and the California Courts Technology Center.
- *Badges and Access*—Managed the AOC badge and access program to protect the AOC’s court visitors, staff, and work for the branch, maintaining badges for AOC employees, temporary staff, consultants, interns, and council and advising the courts upon request. As AOC headquarters is housed in the same facility as the Supreme Court and First Appellate District, OERS shared expertise and support and suggested a no-cost solution to provide the courts with greater transparency and control over their secure areas.
- *Emergency Response*—Managed the AOC Emergency Response Team, training over 100 volunteers to aid in guiding the AOC’s court visitors and staff to evacuate or shelter in place during emergencies in the AOC’s headquarters and regional offices. This requires coordination of over a dozen evacuation rendezvous points and shelter in place locations. As the AOC’s headquarters also houses the Judicial Council Board Room, the OERS works closely with the conference centers to protect the AOC’s visitors and staff.
- *Emergency Equipment*—Helped the AOC meet legal obligations to provide and maintain a safe workplace for staff by providing defibrillators, first aid kits, and emergency kits. OERS took on the Automated External Defibrillation Program per the AOC’s Illness and Injury Prevention Program to meet related training standards and program requirements. It also tracked and maintained hundreds of pieces of emergency equipment in the AOC’s headquarters and regional offices for the protection of the AOC’s court visitors and staff.

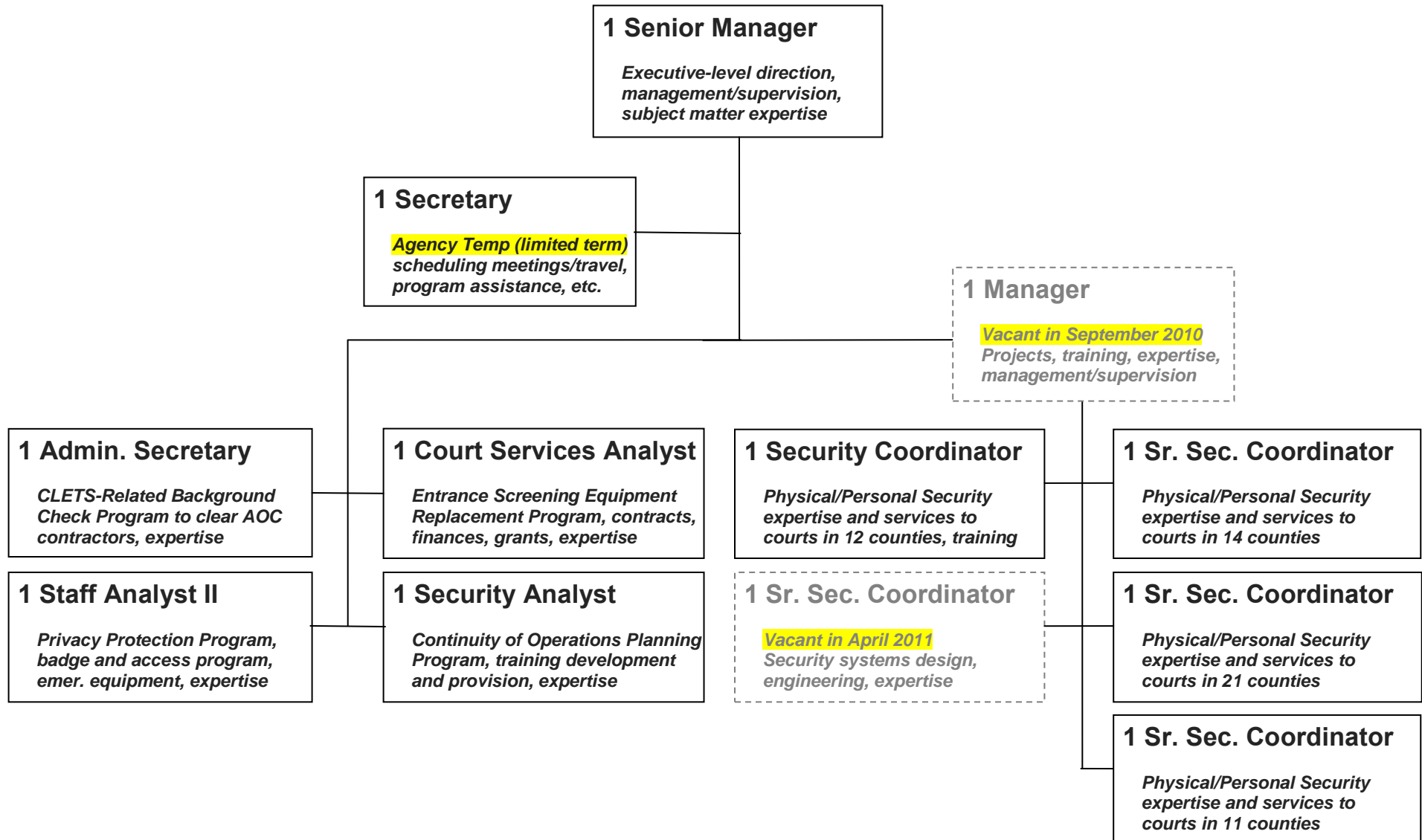
- *Subject Matter Expertise*—Provided expertise and information to many courts, advisory groups, and staff as well as other agencies nationwide, such as presenting security-related coursework as guest speakers at the California Judicial College, assisting the trial courts with security-related presentations to the sheriff and county board of supervisors, providing crime prevention courses to the courts, providing safety compliance courses for the AOC, acting as faculty member at National Center for State Courts events, and more.
- *Resources and Contacts*—Provided information and tools for the courts and AOC such as fact sheets, guidance, brochures, templates, and trainings. Shared and maintained these resources on websites such as Serranus and the AOC Intranet. Created a Fact Sheet and a Programs and Services Update to provide current, convenient sources of information for the judicial branch community about OERS offerings and how to get in touch with staff. Contacted court and AOC staff personally whenever possible to communicate.

III. Status of Current Projects and Initiatives

1. All of the work summarized in the last five pages is ongoing and continues to require work on development, provision, management, and/or maintenance.
2. The OERS is at peak performance level—it has the capacity to cope with emergencies but has no spare capacity for additional tasks. By necessity, the focus of OERS must currently be on the continuation of existing programs and services.
3. The OERS is also trying to complete work on a few high-priority projects and initiatives to address court needs and requests for assistance in an effective manner. These include:
 - Training and guidance to help trial courts with complex x-ray machine registration and training requirements that they must follow by law and to protect court visitors and staff.
 - Changes to the way OERS handles the Judicial Privacy Protection Opt Out Program to make it more convenient for judicial officers, make it more effective, and streamline it.
 - Continued attempts to reduce conflicting workload demands where possible, to address sustained high workloads of OERS staff that handle many programs and services at once.

IV. Division Outlook and Prospective Opportunities, Challenges and Pending Issues

1. As summarized in Sections I through III, the 9 members of the OERS team provide a great deal of advice, assistance, programs, services, trainings, tools, educational materials, and more—and the focus of the unit for the foreseeable future must be on maintaining those existing offerings.
2. The majority of requests for assistance are from the trial courts, and much of the work that OERS does supports the 30+ small courts that do not have subject matter experts in physical security, personal security, and emergency management. Interaction with the appellate courts is, however, limited due to lack of resources and if that changed in the future, OERS could be more involved.
3. The biggest challenges OERS has are maintaining the current level of service that we provide to the trial courts and consolidating services provided to the courts for cost and service efficiencies.



Expenditure Summary ¹	FY 2006-07	FY 2007-08	Annual Percentage Change	FY 2008-09	Annual Percentage Change	FY 2009-10	Annual Percentage Change	FY 2010-11	Annual Percentage Change	Percentage Change FY 2006-07 to FY 2010-11
SUPPORT EXPENDITURES										
Personal Services										
Salaries and Wages	\$ 463,004	\$ 637,622	37.7%	\$ 906,174	42.1%	\$ 972,290	7.3%	\$ 926,143	-4.7%	100.0%
Benefits	158,351	205,318	29.7%	291,559	42.0%	296,602	1.7%	309,898	4.5%	95.7%
Subtotal Personal Services	\$ 621,355	\$ 842,941	35.7%	\$ 1,197,734	42.1%	\$ 1,268,892	5.9%	\$ 1,236,041	-2.6%	98.9%
Operating Expense & Equipment (OE&E)										
Rent	\$ 91,237	\$ 133,932	46.8%	\$ 155,683	16.2%	\$ 155,520	-0.1%	\$ 167,217	7.5%	83.3%
OE&E (Excludes Rent)	741,501	242,504	-67.3%	192,762	-20.5%	261,199	35.5%	212,650	-18.6%	-71.3%
Subtotal OE&E	\$ 832,738	\$ 376,436	-54.8%	\$ 348,445	-7.4%	\$ 416,719	19.6%	\$ 379,867	-8.8%	-54.4%
TOTAL SUPPORT EXPENDITURES	\$ 1,454,093	\$ 1,219,377	-16.1%	\$ 1,546,179	26.8%	\$ 1,685,611	9.0%	\$ 1,615,908	-4.1%	11.1%
Local Assistance	2,693,422	6,784,682	151.9%	2,951,441	-56.5%	2,098,302	-28.9%	1,637,066	-22.0%	-39.2%
TOTAL EXPENDITURES	\$ 4,147,515	\$ 8,004,059	93.0%	\$ 4,497,620	-43.8%	\$ 3,783,913	-15.9%	\$ 3,252,974	-14.0%	-21.6%

Fund Source ¹	FY 2006-07	FY 2007-08	Annual Percentage Change	FY 2008-09	Annual Percentage Change	FY 2009-10	Annual Percentage Change	FY 2010-11	Annual Percentage Change	Percentage Change FY 2006-07 to FY 2010-11
GENERAL FUND & SPECIAL FUNDS										
General Fund	\$ 517,233	\$ 475,313	-8.1%	\$ 438,601	-7.7%	\$ 598,106	36.4%	\$ 505,837	-15.4%	-2.2%
State Court Facilities Trust Fund	735,563	744,064	1.2%	1,107,578	48.9%	1,087,504	-1.8%	1,110,072	2.1%	50.9%
Reimbursements	201,296	-	-100.0%	-	0.0%	-	0.0%	-	0.0%	-100.0%
Subtotal General Fund & Special Funds	\$ 1,454,092	\$ 1,219,377	-16.1%	\$ 1,546,179	26.8%	\$ 1,685,611	9.0%	\$ 1,615,909	-4.1%	11.1%
LOCAL ASSISTANCE										
Trial Court Improvement Fund ²	\$ 1,855,839	\$ 6,784,682	265.6%	\$ 2,951,441	-56.5%	\$ 2,098,302	-28.9%	\$ 1,637,066	-22.0%	-11.8%
Trial Court Trust Fund ³	837,583	-	-100.0%	-	0.0%	-	0.0%	-	0.0%	-100.0%
Subtotal Local Assistance	\$ 2,693,422	\$ 6,784,682	151.9%	\$ 2,951,441	-56.5%	\$ 2,098,302	-28.9%	\$ 1,637,066	-22.0%	-39.2%
TOTAL EXPENDITURES - ALL FUNDS	\$ 4,147,514	\$ 8,004,059	93.0%	\$ 4,497,620	-43.8%	\$ 3,783,913	-15.9%	\$ 3,252,975	-14.0%	-21.6%

⁽¹⁾Source: AOC Financial Forecast Report, prior year actuals.

Local Assistance Expenditures Detail by Fund Source and Program/Project	FY 2006-07	FY 2007-08	Annual Percentage Change	FY 2008-09	Annual Percentage Change	FY 2009-10	Annual Percentage Change	FY 2010-11	Annual Percentage Change	Percentage Change FY 2006-07 to FY 2010-11
<i>Trial Court Improvement Fund</i>										
Trial Court Security Grants ¹	\$ 1,855,839	\$ 6,784,682	265.6%	\$ 2,951,441	-56.5%	\$ 2,098,302	-28.9%	\$ 1,637,066	-22.0%	-11.8%
<i>Subtotal, Trial Court Improvement Fund</i>	\$ 1,855,839	\$ 6,784,682	265.6%	\$ 2,951,441	-56.5%	\$ 2,098,302	-28.9%	\$ 1,637,066	-22.0%	-11.8%
<i>Trial Court Trust Fund</i> ²										
Screening Station Replacement Program	\$ 837,583	\$ -	-100.0%	\$ -	0.0%	\$ -	0.0%	\$ -	0.0%	-100.0%
<i>Subtotal, Trial Court Trust Fund</i>	\$ 837,583	\$ -	-100.0%	\$ -	0.0%	\$ -	0.0%	\$ -	0.0%	-100.0%
TOTAL LOCAL ASSISTANCE FUNDING	\$ 2,693,422	\$ 6,784,682	151.9%	\$ 2,951,441	-56.5%	\$ 2,098,302	-28.9%	\$ 1,637,066	-22.0%	-39.2%

¹The displayed numbers for all fiscal years are from the Oracle Financial, and include the expenditures and encumbrances that are reported on the year-end financial statements.

²TCTF local assistance reflects year-end expenditures and encumbrances recorded in Oracle. After FY 2006-2007, this became a reimbursement program with the funds allocated to the courts.

To: Brandlin, Jim
From: Muffler, John (USMS)
Sent: June 4, 2012 5:12 PM

Judge

I have been trying to pull some specific numbers for you on threats to our protectees, protective details, and weapons confiscated at point of entry screening but it is taking some time to retrieve. I do not think I will have what I want by tomorrow. In the interim I can tell you that the USMS has over 18,000 protective intelligence cases (threats and inappropriate communications) in our data base. In FY 2011 we had 1258 inappropriate communications and in the last 5 years there were 5, 332. Four of our judges were murdered-all at home, all away from the secured environment of the courthouse. One judges family, Judge Joan Lefkow, whom you were empaneled with at the 2011 National Sheriff's Conference in St. Louis, lost her husband and mother to an assassin, a pro se litigant, in the basement of her home. That assassin later committed suicide in the vicinity of another judge's residence while a fugitive from justice.

In the internet age the availability of personal information-home address, kids after school schedule-is at anyone's fingertips. Threateners change targets and cross jurisdiction's-from legislators to judges-in order to be heard and to change their plight. This is a fact and has been proven time and again in studies by law enforcement agencies and academics.

Trained, professional personnel with expertise in risk management, protective investigations and emergency preparedness are essential to sustaining our rule of law in the United States. Protecting judges, legislators and public safety officials is an inherent part of our democracy and ensures our system of justice is fair and impartial. Untrained individuals in these disciplines would not be able to provide the required level of protection rightly needed. The United States Marshals Service provides protective details to threatened officials after careful examination of the threat information. Security details are maintained until the threat is mitigated by operational and administrative professionals in law enforcement and intelligence, respectively. At no time is untrained staff or non-Marshals Service employees-part of this mitigation process; nor should it be left to untrained individuals to make a life or death call on a threat or to evaluate risk.

California is a progressive state in the realm of privacy protection laws. If the other 49 were as good as California we would be a much safer democracy. In fact, I wish the federal laws were as progressive as California as you are truly the pioneer.

If I can be of further assistance please do not hesitate to reach out.

Regards,

John F. Muffler, Administrator
National Center for Judicial Security
United States Marshals Service

Attachment D

Summary of Advisory Groups Addressing Court Security Issues June 12, 2009

1. Appellate Court Security Committee

This committee was established in 1993 by Chief Justice Lucas and was asked to “address state-wide security standards and staffing levels and develop a process to implement local security plans” and to “study and make recommendations regarding security needs for our branch.” The committee worked with the California Highway Patrol and developed an Appellate Court Security program, which commenced in 1996. It is staffed by the California Highway Patrol and is named the “Judicial Protection Section.”

The committee meets annually and by phone and email to address appellate court security issues and to make recommendations to improve security in the appellate courts.

The membership of the committee consists of:

- (1) The Administrative Director of the Courts;
- (2) The Chief Deputy Director of the Courts;
- (3) A Justice representing each of the six Courts of Appeal;
- (4) The Clerk of the Supreme Court;
- (5) A Clerk of the Appellate Court;
- (6) California Highway Patrol representatives; and
- (7) AOC representatives.

The Honorable Patricia Bamattre-Manoukian, Associate Justice of the Court of Appeal, Sixth Appellate District, has chaired the committee since its inception. The Office of Emergency Response and Security provides staff support for the committee.

2. Working Group on Court Security (WGCS)

The Working Group on Court Security (WGCS) was established in 2003 by rule 10.170¹ of the California Rules of Court as required by Government Code section 69927(a)(2). The purpose of the WGCS is to

promulgate recommended uniform standards and guidelines that may be used by the Judicial Council and any sheriff or marshal for the implementation of trial court security services. . . . The Judicial Council, after requesting and receiving recommendations from the working group on court security, shall promulgate and

¹ Rule 10.170 was originally adopted as rule 6.170, but was renumbered in 2007 as part of the reorganization of the California Rules of Court.

implement rules, standards, and policy directions for the trial courts in order to achieve efficiencies that will reduce operating costs and constrain growth in those costs.²

Government Code section 69927(a)(2) specifies that the WGCS consists of an unspecified number of representatives from various groups. California Rules of Court, rule 10.170(b) specifies how many members of the WGCS are appointed by each group:

- (1) Eight representatives from the judicial branch;
- (2) Three representatives from the California State Sheriffs' Association;
- (3) Two representatives from the California State Association of Counties;
- (4) One representative from the Peace Officers' Research Association of California; and
- (5) One representative from the California Coalition of Law Enforcement Associations.

The Chief Justice selects the eight representatives from the judicial branch³ and may appoint an appellate justice as nonvoting chair.⁴ The Honorable Richard D. Aldrich, Associate Justice of the Court of Appeal, Second Appellate District, Third Division, has been the chair of the Working Group on Court Security since its inception.

The AOC Finance Division and the AOC Office of Emergency Response and Security have provided staff support to the WGCS.

The WGCS makes recommendations and reports to the Judicial Council.

3. Working Group on Court Security Fiscal Guidelines (WGCS-FG)

The Working Group on Court Security Fiscal Guidelines (WGCS-FG) was established in 2003 by rule 10.171⁵ of the California Rules of Court as required by Government Code section 69927(a)(1). The purpose of the WGCS-FG is to “recommend modifications only to the template used to determine that the security costs submitted by the courts to the Administrative Office of the Courts are permitted pursuant to this article.” Government Code section 69927(a)(5) states that it may also “periodically recommend changes to the limit for allowable costs for professional support staff for court security operations based on surveys of actual expenditures incurred by trial courts and the court law enforcement provider in the provision of law enforcement security personnel services.”

Government Code section 69927(a)(1) and California Rules of Court, rule 10.171(b) specify the membership of the WGCS-FG. The composition of the group changes if “the working group determines that there is a need to make recommendations to the template that specifically involve

² Gov. Code, § 69927(a)(2).

³ Cal. Rules of Court, rule 10.170(b)(1).

⁴ Cal. Rules of Court, rule 10.170(c).

⁵ Rule 10.171 was originally adopted as rule 6.171, but was renumbered in 2007 as part of the reorganization of the California Rules of Court.

law enforcement or security personnel in courtrooms or court detention facilities. . . .”⁶ When performing allowable costs review and template review, except personnel template review, the WGCS-FG is composed as follows:

- (1) Six representatives from the judicial branch from the WGCS established in California Rules of Court, rule 10.170, as selected by the Administrative Director of the Courts;
- (2) The two representatives of the counties from the WGCS established in California Rules of Court, rule 10.170; and
- (3) The three representatives of the county sheriffs from the WGCS established in California Rules of Court, rule 10.170.⁷

When performing template review involving law enforcement or security personnel costs, the WGCS-FG is composed as follows:

- (1) The same six representatives from the judicial branch of government selected by the Administrative Director of the Courts;
- (2) The same two representatives of the counties;
- (3) Two of the three representatives of the county sheriffs as determined by the California State Sheriffs' Association; and
- (4) Two representatives of labor selected by the California Coalition of Law Enforcement Associations.⁸

The Administrative Director of the Courts may appoint one of the judicial branch members as chair of the WGCS-FG.⁹ The Director of the AOC’s Finance Division has chaired the Working Group on Court Security Fiscal Guidelines since its inception.

Because the membership of the Working Group on Court Security Fiscal Guidelines is drawn, for the most part,¹⁰ from the membership of the Working Group on Court Security, the two groups typically met together and discussed matters as one group.

The AOC Finance Division and the AOC Office of Emergency Response and Security have provided staff support to the WGCS-FG.

The WGCS-FG makes recommendations to and reports to the Judicial Council.

⁶ Gov. Code, § 69927(a)(1).

⁷ Gov. Code, § 69927(a)(1), Cal. Rules of Court, rule 10.171(b)(1).

⁸ Gov. Code, § 69927(a)(1), Cal. Rules of Court, rule 10.171(b)(2).

⁹ Cal. Rules of Court, rule 10.171(c).

¹⁰ Although the judicial branch, county, and sheriff representatives are all drawn from the members of the WGCS, the WGCS-FG includes two members appointed by the California Coalition of Law Enforcement Associations, one more than is appointed to the WGCS.

4. Court Security Education Committee

This committee worked with staff and faculty to develop curriculum and programs statewide for court security training, bringing court security personnel together to share information and learn about specific areas of court security policies and procedures. The committee reported to the Governing Committee of Center for Judicial Education and Research (CJER), before the Governing Committee of CJER disbanded the Court Security Education Committee effective December 31, 2009, as part of a general reorganization of education committees.

5. Ad Hoc Committees on Court Security

Since 2007, a number of ad hoc committees have been formed to address a variety of topics. Ad Hoc Committee have been formed as needed on specific topics. Examples include:

- The Person Security Ad Hoc Advisory Group (2006-2007), which sponsored the OERS survey of California’s judicial officers regarding threats (see Attachment “E” to this report.)
- Ad Hoc Working Group on Court Security (2007-2009), 3. Ad Hoc Working Group on Court Security—This was established on February 20, 2007, which worked on proposals for increasing funding for court security.
- Ad Hoc Working Group on Court Security Realignment (2011-2012), which met with the California Department of Finance regarding the realignment of court security, and has prepared and reviewed proposals for legislation to implement realignment.



ADMINISTRATIVE OFFICE
OF THE COURTS
455 Golden Gate Avenue
San Francisco, CA
94102-3688
Tel 415-865-4200
TDD 415-865-4272
Fax 415-865-4205
www.courtinfo.ca.gov

FACT SHEET

December 2007

Personal Security for Judges and Justices

In January 2007, the Administrative Office of the Courts (AOCs), Emergency Response and Security (ERS) unit conducted a statewide survey of judges and justices to obtain information concerning threats received between December 2005 and December 2006 and to determine current levels of confidence in their safety inside and outside of the courts.

Overview

In the first study of its kind conducted in California, 35 percent of the judges and justices responding to a survey said they were threatened during the course of their work. Three-quarters of the reported threats were made against a specific judicial officer or employee, and most of the threats were made in the courtroom or court chambers. The threats were predominately related to criminal cases, followed by family law cases.

Methodology

The survey was conducted via the Internet and announced to judges and justices via e-mail, newsletter, and Serranus. It reached a total of 1,609 active judges and justices (7 Supreme Court justices, 105 Court of Appeal justices, and 1,497 superior court judges) and achieved an overall response rate of approximately 53 percent, with 855 completed questionnaires. At least one response was received from almost every court—92 percent of the courts were represented in some way—reporting a total of 296 threats.

Survey Findings

Survey findings include the following:

- Of the 296 total threats reported, 72 were described as imminent (about to happen or threatening to happen).
- Seventy-five percent of the total threats reported were against a specific judge, justice, commissioner, referee, employee, or family member. The majority of

these threats were received via oral or written communication. The location most threats were received in was in the courtroom or court chambers.

- Sixty-two percent of the threats were classified as general rather than imminent. When threats were related to a case, those cases were predominately criminal, followed by family law cases. Over half the time, the plaintiff or defendant in the case was the person to make the threat.
- Eighty-three percent of the total threats were reported, most often to the sheriff. The most common precaution taken was to notify courthouse security or staff.
- Eighty-five percent of the judges and justices said the threat had been investigated to their satisfaction, and 79 percent reported that they received feedback about the investigation from the person the threats were reported to.
- Many judges and justices reported being threatened at their residences, where they are often without protection. Over half of the respondents do not have a functioning alarm system at home, and many that do have them do not use them.
- Many judges and justices commented that they were threatened right outside of the courthouse—e.g., in shared parking areas where perimeter security could make a huge difference. Some also expressed concerns about security personnel—i.e., the role that law enforcement plays in regard to threats and the lack of sufficient bailiffs in the courtrooms. Sixteen percent of the respondents carry a concealed weapon.
- Ninety-four percent of the respondents said they feel safe in their homes; 92 percent said they feel safe on the bench; and 87 percent say they feel safe in the court.

The survey results can be found on the Web site listed under “Additional Resources.”

How Will the Findings Be Used?

While the California Highway Patrol does have a system for elected officials and justices, no centralized reporting system exists for threats made against judges. The survey results will assist ERS in examining the personal security issues faced by California’s judges and justices.

Continuing Efforts

ERS will continue its efforts to understand and improve safety and security in the California courts. Work has been completed to remove judges and justices’ personal

information from Internet databases, to assist in the procurement of screening station equipment, and to provide on site physical security surveys for the courts upon request.

As support to several security-related committees and groups, ERS may continue to conduct periodic surveys to measure progress and propose actions that will ensure the highest possible level of personal security for judges and justices.

Contact:

AOC Emergency Response and Security, 415-865-8991, or ers@jud.ca.gov

Additional Resources:

The Personal Security Survey is available at <http://serranus.courtinfo.ca.gov/programs/security/>

A companion fact sheet, "Court Security," provides an overview of other security-related efforts and is available at <http://serranus.courtinfo.ca.gov/programs/security/> and www.courtinfo.ca.gov/reference/documents/factsheets/CourtSecurity.pdf



Personal Security Survey for Judges and Justices

Survey Date: January 2007
Survey Period: December 2005–2006
Project Manager: AOC Emergency Response and Security

Survey Description:

The Personal Security Survey for Judges and Justices will assist the Administrative Office of the Courts' Personal Security Ad Hoc Advisory Group in examining the personal security issues faced by California's judges and justices.

The survey was published using online survey software and distributed to a total of 1,609 active judicial officers (7 Supreme Court justices, 105 Court of Appeal justices, and 1,497 superior court judges). The survey's purpose was to gather information from a large group of judges and justices about the threats they received within the last 12 months. The overall response rate was approximately 53 percent, with 855 completed questionnaires.

The majority of questions were quantitative to collect totals and percentages, which are shown in the responses below. Responses of "other" were evaluated and assigned to the existing categories where possible. Remaining "other" responses were unassignable or not specified.

Readers should note that not all questions were answered by all respondents, and some threats crossed multiple categories. The survey focused on gathering breadth rather than depth of information, and in future surveys questions will be clarified to gather precise statistics.

Questionnaire Responses:

ID	Question	Response
1	N/A	(This question collected information about what county the response was from, for internal tracking purposes only.)

ID	Question	Response																											
2	How many threats did respondents receive in the last 12 months?	<p>The total threats that respondents received were 296. The most threats received by a single respondent was 12.</p> <table border="1"> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Threats</i></th> </tr> </thead> <tbody> <tr> <td>665</td> <td>78%</td> <td>0</td> </tr> <tr> <td>129</td> <td>15%</td> <td>1</td> </tr> <tr> <td>42</td> <td>5%</td> <td>2</td> </tr> <tr> <td>19</td> <td>2%</td> <td>3 or more</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Threats</i>	665	78%	0	129	15%	1	42	5%	2	19	2%	3 or more												
<i>Respondents</i>	<i>Percentage</i>	<i>Threats</i>																											
665	78%	0																											
129	15%	1																											
42	5%	2																											
19	2%	3 or more																											
3	What category were the threats in?	<p>75 percent of the threats were against a specific judge, justice, commissioner, or family member.</p> <table border="1"> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Threat Against</i></th> </tr> </thead> <tbody> <tr> <td>212</td> <td>75%</td> <td>Judge, justice, commissioner, family member</td> </tr> <tr> <td>33</td> <td>12%</td> <td>Generic or unspecified</td> </tr> <tr> <td>18</td> <td>6%</td> <td>Facility/building</td> </tr> <tr> <td>11</td> <td>4%</td> <td>Court staff</td> </tr> <tr> <td>8</td> <td>3%</td> <td>Court system</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Threat Against</i>	212	75%	Judge, justice, commissioner, family member	33	12%	Generic or unspecified	18	6%	Facility/building	11	4%	Court staff	8	3%	Court system									
<i>Respondents</i>	<i>Percentage</i>	<i>Threat Against</i>																											
212	75%	Judge, justice, commissioner, family member																											
33	12%	Generic or unspecified																											
18	6%	Facility/building																											
11	4%	Court staff																											
8	3%	Court system																											
4	How were the threats received?	<p>The majority of threats were received via oral or written communication.</p> <table border="1"> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Received Via</i></th> </tr> </thead> <tbody> <tr> <td>104</td> <td>39%</td> <td>Oral communication</td> </tr> <tr> <td>91</td> <td>34%</td> <td>Written communication</td> </tr> <tr> <td>50</td> <td>19%</td> <td>Third-party contact</td> </tr> <tr> <td>14</td> <td>5%</td> <td>E-mail or electronic media</td> </tr> <tr> <td>7</td> <td>3%</td> <td>Other</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Received Via</i>	104	39%	Oral communication	91	34%	Written communication	50	19%	Third-party contact	14	5%	E-mail or electronic media	7	3%	Other									
<i>Respondents</i>	<i>Percentage</i>	<i>Received Via</i>																											
104	39%	Oral communication																											
91	34%	Written communication																											
50	19%	Third-party contact																											
14	5%	E-mail or electronic media																											
7	3%	Other																											
5	In what location were the threats received?	<p>The location most threats were received in was the courtroom or court chambers.</p> <table border="1"> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Location</i></th> </tr> </thead> <tbody> <tr> <td>107</td> <td>37%</td> <td>Other</td> </tr> <tr> <td>99</td> <td>34%</td> <td>Courtroom</td> </tr> <tr> <td>54</td> <td>19%</td> <td>Court chambers</td> </tr> <tr> <td>24</td> <td>8%</td> <td>Residence</td> </tr> <tr> <td>4</td> <td>1%</td> <td>Court parking lot</td> </tr> </tbody> </table> <p>A further breakdown of responses of "other" revealed these common locations.</p> <table border="1"> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Location</i></th> </tr> </thead> <tbody> <tr> <td>50</td> <td>47% of "other"</td> <td>Courthouse</td> </tr> <tr> <td>18</td> <td>17% of "other"</td> <td>Community</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Location</i>	107	37%	Other	99	34%	Courtroom	54	19%	Court chambers	24	8%	Residence	4	1%	Court parking lot	<i>Respondents</i>	<i>Percentage</i>	<i>Location</i>	50	47% of "other"	Courthouse	18	17% of "other"	Community
<i>Respondents</i>	<i>Percentage</i>	<i>Location</i>																											
107	37%	Other																											
99	34%	Courtroom																											
54	19%	Court chambers																											
24	8%	Residence																											
4	1%	Court parking lot																											
<i>Respondents</i>	<i>Percentage</i>	<i>Location</i>																											
50	47% of "other"	Courthouse																											
18	17% of "other"	Community																											

ID	Question	Response																								
6	How do respondents classify the threats?	<p>Of the 296 total threats reported, 72 were described as imminent (about to happen or threatening to happen).</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Classification</i></th> </tr> </thead> <tbody> <tr> <td>201</td> <td>69%</td> <td>General</td> </tr> <tr> <td>72</td> <td>25%</td> <td>Imminent</td> </tr> <tr> <td>18</td> <td>6%</td> <td>Other</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Classification</i>	201	69%	General	72	25%	Imminent	18	6%	Other												
<i>Respondents</i>	<i>Percentage</i>	<i>Classification</i>																								
201	69%	General																								
72	25%	Imminent																								
18	6%	Other																								
7	If the threats were related to cases, what kind of cases were they?	<p>Threats were predominately related to criminal cases.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Case</i></th> </tr> </thead> <tbody> <tr> <td>122</td> <td>45%</td> <td>Criminal</td> </tr> <tr> <td>77</td> <td>29%</td> <td>Family</td> </tr> <tr> <td>36</td> <td>14%</td> <td>Civil</td> </tr> <tr> <td>29</td> <td>11%</td> <td>Other</td> </tr> <tr> <td>5</td> <td>2%</td> <td>Traffic</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Case</i>	122	45%	Criminal	77	29%	Family	36	14%	Civil	29	11%	Other	5	2%	Traffic						
<i>Respondents</i>	<i>Percentage</i>	<i>Case</i>																								
122	45%	Criminal																								
77	29%	Family																								
36	14%	Civil																								
29	11%	Other																								
5	2%	Traffic																								
8	Who were the threats made by?	<p>Over half the time, the plaintiff or defendant was the person to make the threat.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Threat from</i></th> </tr> </thead> <tbody> <tr> <td>173</td> <td>60%</td> <td>Plaintiff or defendant</td> </tr> <tr> <td>40</td> <td>14%</td> <td>Unknown</td> </tr> <tr> <td>29</td> <td>10%</td> <td>Other</td> </tr> <tr> <td>27</td> <td>9%</td> <td>In-custody inmate</td> </tr> <tr> <td>18</td> <td>6%</td> <td>Family of plaintiff or defendant</td> </tr> <tr> <td>2</td> <td>1%</td> <td>Counsel</td> </tr> <tr> <td>0</td> <td>0%</td> <td>Court employee</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Threat from</i>	173	60%	Plaintiff or defendant	40	14%	Unknown	29	10%	Other	27	9%	In-custody inmate	18	6%	Family of plaintiff or defendant	2	1%	Counsel	0	0%	Court employee
<i>Respondents</i>	<i>Percentage</i>	<i>Threat from</i>																								
173	60%	Plaintiff or defendant																								
40	14%	Unknown																								
29	10%	Other																								
27	9%	In-custody inmate																								
18	6%	Family of plaintiff or defendant																								
2	1%	Counsel																								
0	0%	Court employee																								
9	Were the threats reported?	<p>80 percent of the total threats were reported.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Reported</i></th> </tr> </thead> <tbody> <tr> <td>236</td> <td>80%</td> <td>Yes</td> </tr> <tr> <td>48</td> <td>16%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Reported</i>	236	80%	Yes	48	16%	No															
<i>Respondents</i>	<i>Percentage</i>	<i>Reported</i>																								
236	80%	Yes																								
48	16%	No																								
10	If so, who were the threats reported to?	<p>Threats were reported most often to the sheriff.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Reported to</i></th> </tr> </thead> <tbody> <tr> <td>180</td> <td>72%</td> <td>Sheriff</td> </tr> <tr> <td>34</td> <td>14%</td> <td>Other</td> </tr> <tr> <td>24</td> <td>10%</td> <td>Police</td> </tr> <tr> <td>8</td> <td>3%</td> <td>CHP</td> </tr> <tr> <td>4</td> <td>2%</td> <td>District attorney</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Reported to</i>	180	72%	Sheriff	34	14%	Other	24	10%	Police	8	3%	CHP	4	2%	District attorney						
<i>Respondents</i>	<i>Percentage</i>	<i>Reported to</i>																								
180	72%	Sheriff																								
34	14%	Other																								
24	10%	Police																								
8	3%	CHP																								
4	2%	District attorney																								
11	Were the threats investigated to the respondents' satisfaction?	<p>85 percent of respondents who reported threats were satisfied with the investigation.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>209</td> <td>85%</td> <td>Yes</td> </tr> <tr> <td>37</td> <td>15%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	209	85%	Yes	37	15%	No															
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																								
209	85%	Yes																								
37	15%	No																								

ID	Question	Response																								
12	Did respondents receive feedback about the status of the investigations?	<p>79 percent of respondents who reported threats received feedback about the status of the investigation from the person the threats were reported to.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Received</i></th> </tr> </thead> <tbody> <tr> <td>197</td> <td>79%</td> <td>Yes</td> </tr> <tr> <td>52</td> <td>21%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Received</i>	197	79%	Yes	52	21%	No															
<i>Respondents</i>	<i>Percentage</i>	<i>Received</i>																								
197	79%	Yes																								
52	21%	No																								
13	What precautions were taken as a result?	<p>The most common precaution taken was to notify courthouse security or staff.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Actions</i></th> </tr> </thead> <tbody> <tr> <td>76</td> <td>30%</td> <td>Other</td> </tr> <tr> <td>126</td> <td>49%</td> <td>Told courthouse security/staff</td> </tr> <tr> <td>18</td> <td>7%</td> <td>Briefed family</td> </tr> <tr> <td>15</td> <td>6%</td> <td>Changed home security system</td> </tr> <tr> <td>11</td> <td>4%</td> <td>Changed courthouse perimeter screening</td> </tr> <tr> <td>6</td> <td>2%</td> <td>Got security escort</td> </tr> <tr> <td>3</td> <td>1%</td> <td>Changed courthouse parking area</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Actions</i>	76	30%	Other	126	49%	Told courthouse security/staff	18	7%	Briefed family	15	6%	Changed home security system	11	4%	Changed courthouse perimeter screening	6	2%	Got security escort	3	1%	Changed courthouse parking area
<i>Respondents</i>	<i>Percentage</i>	<i>Actions</i>																								
76	30%	Other																								
126	49%	Told courthouse security/staff																								
18	7%	Briefed family																								
15	6%	Changed home security system																								
11	4%	Changed courthouse perimeter screening																								
6	2%	Got security escort																								
3	1%	Changed courthouse parking area																								
14	N/A	(This question was a hyperlink that allowed respondents to enter information about additional threats received.)																								
15	What significant threats have respondents received in the last five years that will assist us in seeing a larger picture with the state of threat to the judiciary?	<p>A wide variety of comments were received. The majority gave additional facts about threats that they had received, while others offered opinions about threats to the judiciary.</p> <p>Many judicial officers reported being threatened at their residences, where they are often without protection.</p> <p>Many also commented that they were threatened right outside of the courthouse—e.g., in shared parking areas where perimeter security could make a huge difference.</p> <p>Several respondents indicated that modifications were needed to improve security in their courthouses.</p> <p>Some also specified concerns about security personnel—i.e., the role that law enforcement plays in regard to threats and the lack of sufficient bailiffs in the courtrooms.</p>																								
16	Do respondents use an alarm system at home?	<p>80 percent of respondents do not use an alarm system.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>System</i></th> </tr> </thead> <tbody> <tr> <td>658</td> <td>80%</td> <td>No</td> </tr> <tr> <td>167</td> <td>20%</td> <td>Yes</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>System</i>	658	80%	No	167	20%	Yes															
<i>Respondents</i>	<i>Percentage</i>	<i>System</i>																								
658	80%	No																								
167	20%	Yes																								

ID	Question	Response																		
17	Do respondents have a functioning home intrusion detection system?	<p>403 respondents have functioning alarm systems in their homes, although they may not use them.</p> <p>The remaining respondents either do not have an alarm system or have a nonfunctioning system.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>System</i></th> </tr> </thead> <tbody> <tr> <td>447</td> <td>53%</td> <td>No</td> </tr> <tr> <td>403</td> <td>47%</td> <td>Yes</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>System</i>	447	53%	No	403	47%	Yes									
<i>Respondents</i>	<i>Percentage</i>	<i>System</i>																		
447	53%	No																		
403	47%	Yes																		
18	How long ago was it installed?	<p>The majority of the alarm systems that respondents have are over five years old.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Installed</i></th> </tr> </thead> <tbody> <tr> <td>309</td> <td>76%</td> <td>5 or more years</td> </tr> <tr> <td>28</td> <td>7%</td> <td>1 year</td> </tr> <tr> <td>27</td> <td>7%</td> <td>2 years</td> </tr> <tr> <td>27</td> <td>7%</td> <td>3 years</td> </tr> <tr> <td>17</td> <td>4%</td> <td>4 years</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Installed</i>	309	76%	5 or more years	28	7%	1 year	27	7%	2 years	27	7%	3 years	17	4%	4 years
<i>Respondents</i>	<i>Percentage</i>	<i>Installed</i>																		
309	76%	5 or more years																		
28	7%	1 year																		
27	7%	2 years																		
27	7%	3 years																		
17	4%	4 years																		
19	Is it monitored by a third party?	<p>Over half of the 403 functioning alarm systems that were reported are monitored by a third party.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>340</td> <td>59%</td> <td>Yes</td> </tr> <tr> <td>241</td> <td>41%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	340	59%	Yes	241	41%	No									
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																		
340	59%	Yes																		
241	41%	No																		
20	If available, would respondents use a home alarm service?	<p>Most respondents would use a home alarm service if it was made available to them.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>677</td> <td>87%</td> <td>Yes</td> </tr> <tr> <td>103</td> <td>13%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	677	87%	Yes	103	13%	No									
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																		
677	87%	Yes																		
103	13%	No																		
21	Do respondents plan to move to a different primary residence within the next six months?	<p>Almost all respondents plan to remain in the same primary residence for at least six months.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>798</td> <td>95%</td> <td>No</td> </tr> <tr> <td>39</td> <td>5%</td> <td>Yes</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	798	95%	No	39	5%	Yes									
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																		
798	95%	No																		
39	5%	Yes																		
22	Do respondents carry concealed weapons?	<p>84 percent of respondents do not carry concealed weapons.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>704</td> <td>84%</td> <td>No</td> </tr> <tr> <td>130</td> <td>16%</td> <td>Yes</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	704	84%	No	130	16%	Yes									
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																		
704	84%	No																		
130	16%	Yes																		
23	Do respondents feel safe in their homes?	<p>94 percent of respondents said they feel safe in their homes—slightly more than the number that feel safe on the bench or in the courthouse.</p> <table> <thead> <tr> <th><i>Respondents</i></th> <th><i>Percentage</i></th> <th><i>Response</i></th> </tr> </thead> <tbody> <tr> <td>785</td> <td>94%</td> <td>Yes</td> </tr> <tr> <td>53</td> <td>6%</td> <td>No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	785	94%	Yes	53	6%	No									
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>																		
785	94%	Yes																		
53	6%	No																		

ID	Question	Response									
24	Do respondents feel safe on the bench?	<p>92 percent of respondents said they feel safe on the bench.</p> <table border="0"> <thead> <tr> <th data-bbox="683 348 846 380"><i>Respondents</i></th> <th data-bbox="915 348 1052 380"><i>Percentage</i></th> <th data-bbox="1143 348 1263 380"><i>Response</i></th> </tr> </thead> <tbody> <tr> <td data-bbox="683 380 732 407">776</td> <td data-bbox="915 380 964 407">92%</td> <td data-bbox="1143 380 1192 407">Yes</td> </tr> <tr> <td data-bbox="683 407 716 434">66</td> <td data-bbox="915 407 948 434">8%</td> <td data-bbox="1143 407 1175 434">No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	776	92%	Yes	66	8%	No
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>									
776	92%	Yes									
66	8%	No									
25	Do respondents feel safe in the courthouse?	<p>87 percent of respondents said they feel safe in the courthouse.</p> <table border="0"> <thead> <tr> <th data-bbox="683 543 846 575"><i>Respondents</i></th> <th data-bbox="915 543 1052 575"><i>Percentage</i></th> <th data-bbox="1143 543 1263 575"><i>Response</i></th> </tr> </thead> <tbody> <tr> <td data-bbox="683 575 732 602">735</td> <td data-bbox="915 575 964 602">87%</td> <td data-bbox="1143 575 1192 602">Yes</td> </tr> <tr> <td data-bbox="683 602 732 630">106</td> <td data-bbox="915 602 964 630">13%</td> <td data-bbox="1143 602 1175 630">No</td> </tr> </tbody> </table>	<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>	735	87%	Yes	106	13%	No
<i>Respondents</i>	<i>Percentage</i>	<i>Response</i>									
735	87%	Yes									
106	13%	No									



CONFIDENTIAL
**JUDICIAL PROTECTION SECTION NORTH STATE UNIT
INFORMATION CONTROL REPORT**

TARGET CODE	CASE NUMBER
-------------	-------------

VICTIM NAME

PERSONAL DATA

LAST NAME					FIRST NAME	
RACE	SEX	HEIGHT	WEIGHT	HAIR	EYES	AGE
DOB		SSN	MARITAL		SPOUSE	
STREET		CITY			STATE	
ZIP		DL #	TELEPHONE		COUNTY	
AKA (S)						

FILE INFORMATION

DATE REPORT	DATE OF LAST REPORT	TYPE		LEVEL CODE	
POSTMARK CITY	POSTMARK STATE	OPI ENTRIES	CITY OF OCCURRENCE	COUNTY	
CRIMINAL HISTORY <input type="checkbox"/> YES <input type="checkbox"/> NO	CII NUMBER	FBI NUMBER	CDC NUMBER	OTHER	
VEHICLES	YEAR	MAKE	MODEL	COLOR	LICENSE NUMBER
<input type="checkbox"/> WEAPONS	<input type="checkbox"/> MENTAL HEALTH	<input type="checkbox"/> PAROLEE	<input type="checkbox"/> VIOLENT	<input type="checkbox"/> OTHER	<input type="checkbox"/> MEDICAL

SUMMARY

SUBMITTED BY	ASSIGNED TO	DATE
OFFICER ID	APPROVING SUPERVISOR	DATE

DESTROY BY SHREDDING
(REVISED 05/05)

Attachment G

Original: **California Highway Patrol**
(Local Area Office)

**REPORT OF CRIME/INCIDENT ON STATE PROPERTY
MISSING/LOST PROPERTY**

STD. 99 (REV. 3/2010)

- ORIGINAL REPORT SUPPLEMENTAL REPORT
 MISSING/LOST PROPERTY (Attach copy of STD. 152, Property Survey Report)

- Copy: State Agency Completing/Filling Report
Copy: State Agency Headquarters
Copy: Bureau of State Audits
Copy: Department of Finance (Larceny or Fraud ONLY)

State agencies are required to complete and mail a STD. 99, Report of Crime/Incident on State Property Missing/Lost Property, to their local California Highway Patrol (CHP) office if a crime/incident has occurred on state-owned or state-leased property.

PLEASE TYPE OR PRINT ALL INFORMATION

1A. CRIME DATE (Mo./Day/Yr.)		1B. (If unknown discovery date)		2. CRIME CLASSIFICATION (i.e., Assault, Theft, Vandalism)		3. REPORTING PARTY		
4. AGENCY/DEPARTMENT REPORTING CRIME				5. LOCATION WHERE CRIME OCCURRED (Street Address, City, County, Zip Code)				
6. LOCATION OF REPORTING AGENCY (Street Address, City, County, Zip Code)						7. PHONE NUMBER		
8. WAS A REPORT FILLED WITH LOCAL LAW ENFORCEMENT? (IF CHP RESPONDED, DO NOT SUBMIT SEPARATE STD. 99)							9. CASE NUMBER	
<input type="checkbox"/> YES <input type="checkbox"/> NO		IF YES, NAME OF AGENCY						
10. PERSON (Last Name, First Name, Middle Initial)			Check all applicable boxes:					
			<input type="checkbox"/> VICTIM <input type="checkbox"/> SUSPECT <input type="checkbox"/> WITNESS <input type="checkbox"/> EMPLOYEE <input type="checkbox"/> VISITOR <input type="checkbox"/> UNKNOWN					
PROPERTY INVOLVED								
<input type="checkbox"/> STATE (Building or Property)		<input type="checkbox"/> OTHER (Please describe)						
Workplace Violence								
<input type="checkbox"/> Type I Inappropriate conduct by people with no legitimate business at the workplace								
<input type="checkbox"/> Type II Inappropriate conduct by a customer or client of the workplace								
<input type="checkbox"/> Type III Inappropriate conduct associated to the workplace through an employee								
11. DESCRIBE TYPE OF STATE FACILITY WHERE CRIME OCCURRED (Check all applicable boxes)								
<input type="checkbox"/> STATE-OWNED		<input type="checkbox"/> OFFICE/BUILDING		<input type="checkbox"/> PARKING LOT		<input type="checkbox"/> MAINTENANCE YARD/OPEN LAND		
<input type="checkbox"/> STATE-LEASED		<input type="checkbox"/> WAREHOUSE/STORAGE FACILITY		<input type="checkbox"/> MECHANICAL/UTILITY SHOP		<input type="checkbox"/> OTHER		
12. BRIEF DESCRIPTION/DETAILS OF THE CRIME (Who, What, Where, and How)								

COMPLETE THE FOLLOWING SECTION IF ANY PROPERTY WAS LOST, STOLEN, OR DAMAGED.

NOTE: REFERENCE THE STATE ADMINISTRATIVE MANUAL (SAM) SECTION 8643 FOR INSTRUCTIONS ON COMPLETING THE STD. 152, PROPERTY SURVEY REPORT FORM.

13.	DESCRIBE ALL PROPERTY (Include Brand/Make/Model)	SERIAL NUMBER (If available)	STATE OWNED/LEASED	PRIVATELY OWNED	PROPERTY DAMAGE (Estimated damage value)	PROPERTY LOSS (Estimated loss value)

FOR CHP USE ONLY

If report involves a monetary loss due to burglary, theft, robbery, or vandalism, attach a copy of the completed CHP 729, Uniform Crime Report.

14. AREA-CASE NUMBER		ARRESTING/INVESTIGATING OFFICER		CRIME CLASS SECTION		I.D. NUMBER
FOLLOW-UP ASSIGNED TO				DATE		I.D. NUMBER
REVIEWING SUPERVISOR				DATE		I.D. NUMBER
15. ASSIGNED CATEGORY		16. DISPOSITION CODE	17. CIR CODE	18. DATA ENTRY OPERATOR		I.D. NUMBER
						ENTRY DATE

Commands shall retain copies of the completed STD. 99 along with the corresponding report (i.e., CHP 216 or CHP 202), and the Uniform Crime Report, CHP 729, if applicable, for a period no longer than 3 years.

QUESTIONS REGARDING THE STD. 99 SHOULD BE REFERRED TO STATE SECURITY DIVISION (916) 843-3230.