JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

SP23-03

Title
Facilities Services: Security Systems Program

Action Requested
Review and submit comments by May 25, 2023

Proposed Rules, Forms, Standards, or Statutes
None

Proposed Effective Date
September 27, 2023

Proposed by
Court Security Advisory Committee
Hon. Charlaine F. Olmedo, Chair
Judicial Council staff
Edward Ellestad, Supervisor—Emergency Planning and Security Coordination Unit
Facilities Services

Contact
Li Gotch, 415-865-4365
lisa.gotch@jud.ca.gov

Executive Summary and Origin

In an action by email on April 21, the Court Security Advisory Committee agreed to request public comment on the draft proposed *Judicial Council Policy on Security Systems Program*, with the goal of recommending to the Judicial Council that it adopt the final proposed policy at its September 2023 meeting. Staff presented the draft to the Court Security Advisory Committee in November 2022 to document existing internal procedures, and the committee discussed the benefit of proposing it as a Judicial Council policy at its February 2023 meeting.

Background

Since fiscal year 2019–20, the Security Systems Program has had a budget of $6 million funded annually through the Governor's Budget with which it refreshes, maintains, replaces, improves, and installs electronic security equipment and systems. The program includes (but is not limited to) video surveillance, access control, duress alarm, and specialized systems as well as services to evaluate and design new or replacement systems. It is one of many programs and services provided through the Facilities Services' Emergency Planning and Security Coordination Unit, and the Court Security Advisory Committee has a role in reviewing and approving proposed projects.

The Proposal

The proposed policy documents the Security Systems Program procedures and methodology, for equitable distribution of funds. Its creation is consistent with policies for other Facilities Services programs.

Alternatives Considered

One alternative considered was to continue to follow the current methodology and procedures with the existing internal documentation and Court Security Advisory Committee feedback. However, requesting and reviewing public comment before requesting the Judicial Council's approval of a formal policy will help ensure that practices are well-considered, transparent, and more readily available for reference.

Fiscal and Operational Impacts

Approval of a policy documenting methodology and procedures will incur no costs.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?

The advisory committee also seeks comments from *courts* on the following cost and implementation matters:

- What implementation issues has the Court Security Advisory Committee not yet considered?

Attachments and Links

1. *Judicial Council Policy on Security Systems Program*

DRAFT March 15, 2023

Judicial Council Policy on Security Systems Program

Approved by the Judicial Council on [tbd]

Judicial Council *of* California

Contents

Purpose

Security systems are a critical and integral portion of facility infrastructure. These systems help provide and maintain a safe and secure environment for the public and staff. The Security Systems Program (SSP) was created to maintain court security systems by focusing on replacements and improvements and by updating the existing obsolete technology, giving the Judicial Council of California a greater ability to address threats and reduce vulnerability and associated risks.

Security systems installed and maintained by the SSP include video surveillance, electronic access, wireless duress alarm, and detention control systems in trial courts.

The SSP supports Goals III and VI of the *Strategic Plan for California's Judicial Branch*:

- Goal III: Modernization of Management and Administration states that "the judicial branch must … ensure that court environments are safe and secure."

- Goal VI: Branchwide Infrastructure for Service Excellence states that "the judicial branch must meet the challenge of providing the necessary technological, human resources, fiscal, and facilities infrastructures, as well as other relevant and critical internal functions, to provide the highest quality of justice and service to the people of California." The plan addresses facilities infrastructure improvements specifically, indicating that improvements are needed to "[p]rovide and maintain safe, dignified, and fully functional facilities for conducting court business" and to "[p]rovide judicial branch facilities that accommodate the needs of all court users, as well as those of justice system partners."

Scope

The SSP installs, upgrades, replaces, repairs, and maintains security systems in trial court facilities statewide utilizing competitively bid contracts with security system vendors to provide equipment and services that are generally consistent with *Security Systems Design Criteria Guide* recommendations from the Judicial Council Facilities Services' Emergency Planning and Security Coordination Unit (EPSCU). Product availability, compatibility with existing equipment, and ongoing changes to technology may require solutions outside of those detailed in the guide.

Definitions

- *Install/replace* is:

    - The addition of a system that does not currently exist in the facility; or
    - Replacement of an existing system with one of equal or better quality or function consistent with *Security Systems Design Criteria Guide* and/or consultant recommendations.

- *Upgrade* is the furnishing of specific system components necessary to improve the quality or function of the existing system.

- *Repair/maintain* is action that restores and ensures the continued function of existing systems.

Identification, Prioritization, and Approval of Work

Work to be performed is identified as either planned projects or unplanned/emergency repairs.

Planned Projects

Planned projects install, upgrade, or replace security systems.

Identification

Planned projects are identified by various means, including the following:

- Maintenance history. The need to replace or upgrade systems may be determined based on maintenance history.

- Security systems evaluations. Evaluations are used to identify current system age, condition, technological obsolescence, and estimated remaining life span. These evaluations assist with determining the need and urgency for replacement or upgrade. The evaluations and assessments may be performed by any combination of the following: Judicial Council–contracted consultants, EPSCU staff, and Judicial Council security equipment vendors.

- Court request. Trial courts may request assistance with a project.

- Recent SSP projects. Projects performed in specific courts may be considered for parity.

- Planned major capital improvement. Planned major capital projects that would address the security system need in a reasonable period of time will be a factor in considering the project request and the efficient use of resources. To the extent possible, the existing system will be maintained to keep it functioning until the capital project is completed.

Projects are typically identified by security need, maintenance history, system evaluations, or court requests. In some cases, an unplanned/emergency repair request may be determined to be a planned project.

Process

1. EPSCU prioritizes projects by identifying the security benefit of the project, analyzing maintenance history, evaluations, court requests (including deferred project requests), recent projects in the court, and pending capital projects to determine need and the level of urgency.

2. An EPSCU project manager (PM) sends a *Service Request Form* to one of the contracted vendors to initiate the development of the scope of work (SOW).
3. Stakeholders meet at the site and conduct a walkthrough to discuss the system, court needs, and the extent of the work to be performed. Stakeholders typically include Judicial Council, court, vendor, and security provider staff.
4. The vendor develops the SOW and submits a *Contractor Proposal Form* to the EPSCU PM for review and approval.
5. EPSCU provides a cost-redacted SOW to the court for review and approval and keeps a signed copy on file as part of the project documents.
6. EPSCU staff prioritize potential projects using the *Project Prioritization Scoring Sheet* (Attachment A).
7. EPSCU submits a prioritized list of proposed projects for review, discussion, and approval by the Court Security Advisory Committee either at a regularly scheduled meeting or via an emailed out-of-cycle approval request.
8. EPSCU staff creates service work orders (SWOs) for each approved project and Facilities Modification Identification (FMID) numbers are assigned.[1]
9. EPSCU requests any necessary asbestos-containing materials (ACM) and lead-based paint surveys, and creates a supplemental facility modification SWO for the survey work.
10. SSP funds are encumbered on a purchase order for the project.
11. EPSCU registers the project with the Department of Industrial Relations.
12. EPSCU meets with vendors regularly for planning and project status updates. Vendors and EPSCU staff communicate with the courts to provide updates and discuss the schedule and progress of the projects.
13. EPSCU staff may visit the site while work is in progress, if necessary, and when the work is complete for a commissioning meeting with the vendor and the court.
14. The court completes the *Acceptance and Sign off Form* when the work is complete, and the vendor submits the form with the final project invoice to EPSCU.

A one-year warranty period in addition to any equipment manufacturer warranties is included in the vendor contracts. Vendor provides service visits relating to recently installed or replaced/upgraded systems if necessary.

Following the expiration of the initial one-year warranty period, SSP funds are used to provide service for unplanned/emergency repairs.

---

[1] Security Systems Program contractors working on the council's behalf in the courts, will pass a background check through the internal Contractor Clearance Policy, or be escorted at all times in restricted areas by someone who has.

Unplanned/Emergency Repairs

Trial court or Judicial Council staff submit a SWO outlining the issue and requesting service. The SWO will be assigned to a contracted vendor for response within the contracted time frame and approved costs paid by the SSP. In some cases, emergency repairs or unplanned projects may result in the need for further evaluation and may become a planned project instead.

Project Approval

Per rule 10.61(a) of the California Rules of Court, the charge of the Court Security Advisory Committee is to make recommendations to the council for improving court security, including personal security and emergency response planning.

Projects under consideration for funding by the SSP are presented by EPSCU to the Court Security Advisory Committee or chair for review, discussion, and approval.

All planned projects are subject to available SSP funding.

Limitations on Scope

SSP funds are available only for the purpose described in this policy. These funds are not intended for projects such as the remodeling of clerk counters; the installation of ballistic glass, bollards, or security fencing; or the abatement of asbestos/hazardous material.

Additional details on scope, responsibilities, and exclusions for each type of system follow.

Video Surveillance Systems

Scope of work

1. Evaluate the existing system—including camera positions, coverage, and existing infrastructure—to determine appropriate upgrades to the system, including camera types, resolution, and optimum coverage.
2. Review monitoring/control locations, including ergonomic considerations, required camera views, and display options.
3. Identify any integration between other security system components—including access control, detention control, intercom, and wireless duress alarm systems—and the potential impact of changes to the system.
4. Connect critical components to existing uninterruptible power supply (UPS) systems, or if feasible, provide UPS components as needed.

Components may include cameras, mounting accessories, monitors and workstations, recording servers, cabling, UPS devices, and all licensing required for a complete and functioning system.

Responsibilities

EPSCU

1. Coordinate initial meetings with court, vendor, and Judicial Council contacts.
2. Assist with coordination of ACM and lead-based paint testing between the court and the testing vendor.
3. Include discussion of after-hours access and escorting during the project, if necessary.
4. Facilitate coordination of e-waste disposal.

Vendor

1. Conduct a kickoff meeting explaining the work process and how it may affect the court.
2. Coordinate with the court the scheduling of the work, and determine which areas, if any, will be affected by the project to minimize disruptions.
3. Clean up as work is completed in each area.
4. Control and account for tools in accordance with the existing Facilities Services *Tool Control Policy* as work is done throughout the facility, with increased attention in detention spaces.
5. Coordinate with court information technology (IT) and other court staff for access to space or network resources such as switch ports and internet protocol (IP) addresses.
6. When ACM is present, observe proper Class III certification and practices as required.
7. Program individual or group user access levels to the system as instructed by the court.
8. Provide training on the installed equipment.
9. Provide drawings with sufficient detail to identify device locations, switches, patch panels, headend equipment, and where possible, cable paths.

Court

1. Provide access to vendor employees as necessary to perform the work.
2. Provide key contact information for scheduling work.
3. Provide a staging location for materials and work area.
4. Identify who will provide final review of camera views (usually in conjunction with court security).
5. Provide network connectivity if approved by court IT, along with IP addressing detail as required by the contractor.
6. Identify staff who need to be trained on the equipment, and coordinate with the contractor for training time or sessions.
7. Provide instructions and procedures to facilitate remote access to the system for maintenance and troubleshooting, if approved by court IT.

8. Identify proper user access levels for each user of the system—for example, who can view live and recorded video, who is authorized to download or archive video clips, and who may have full administrative access to the system.
9. Identify who will sign the acceptance form on completion of the work.

Exclusions

- Excluded items include, but are not limited to, millwork, patching and painting, abatement of asbestos or lead-based paint, and the cost of after-hours, weekend, or holiday escort, if required by the court.
- Additional exclusions may be included in specific scopes of work provided by the vendor.

Electronic Access Systems

Scope of work

1. Evaluate existing electronic access needs based on current technology and potential security vulnerability.
2. Identify locations for electronic access control to replace mechanical cypher locks or keyed lock locations that fit with current design criteria standards.
3. Evaluate mechanical and electrified door hardware that could be affected by upgrading the system.
4. Update any existing system hardware and software as needed.
5. Identify any integration between other security components including video, detention control, intercom, and wireless duress alarm systems and the potential impact of changes to the electronic access control systems.
6. Connect critical components to existing UPS systems or provide UPS components as needed.

Components include electrified hardware, request to exit sensors, control panels, workstations, and servers, cabling, UPS devices, and all licensing required for a complete and functioning system.

Responsibilities

EPSCU

1. Coordinate initial meetings with court, vendor, and Judicial Council contacts.
2. Assist with coordination of ACM and lead-based paint testing between the court and the testing vendor.
3. Include discussion of after-hours access and escorting during the project, if necessary.
4. Facilitate coordination of disposal of e-waste and other removed components.

Vendor

1. Conduct a kickoff meeting explaining the work process and how it may affect the court.
2. Coordinate with the court the scheduling of the work, and determine which areas, if any, will be affected by the project to minimize disruptions.
3. Clean up as work is completed in each area.
4. Control and account for tools in accordance with the existing Facilities Services *Tool Control Policy* as work is done throughout the facility, with increased attention in detention spaces.
5. Coordinate with IT and other court staff for access to space or network resources such as switch ports and IP addresses.
6. When ACM is present, observe proper Class III certification and practices, as required.
7. Program individual or group user access levels to the system as instructed by the court.
8. Provide training on the installed equipment.
9. Provide drawings with sufficient detail to identify device locations, switches, patch panels, headend equipment, and where possible, cable paths.

Court

1. Provide access to vendor employees as necessary to perform the work.
2. Provide key contact information for scheduling work and a staging location for materials and the work area.
3. Work with the contractor to identify appropriate locations for door control panels and power supplies.
4. Provide network connectivity if approved by court IT, along with IP addressing detail as required by the contractor.
5. Identify staff who need to be trained on the equipment and administrative access levels for users, and coordinate with the contractor for training.
6. Provide instructions and procedures to facilitate remote access to the system for maintenance and troubleshooting, if approved by court IT.
7. Identify who will sign the acceptance form on completion of the work.

Exclusions

- Excluded items include, but are not limited to, millwork, patching and painting, abatement of asbestos or lead paint, and cost of after-hours, weekend, or holiday escort, if required by the court.
- Additional exclusions may be included in specific scopes of work provided by the vendor.

Wireless Duress Alarm Systems

Scope of work

1. Provide wireless duress buttons and sensors to immediately send notifications of the location of the activation to personnel identified by the court.
2. Include wireless sensors, signal boosters, a central control unit, and a radio communication device.

Responsibilities

EPSCU

1. Coordinate initial meetings with court, vendor, and Judicial Council contacts.
2. Provide information to the court and security on the capability of the system and the advantages of radio communication if the court and security providers are unfamiliar with the concept and application in a court environment.
3. Assist with coordination of ACM and lead-based paint testing between the court and the testing vendor.
4. Include discussion of after-hours access and escorting during the project, if necessary.
5. Facilitate coordination of disposal of e-waste and other removed components.

Vendor

1. Design locations for headend installation and signal booster locations to optimize signal from buttons, ensuring activations are properly received.
2. Test functionality of the system, including all buttons.
3. Provide instructions on maintenance of the system, including testing and identifying when battery replacement is needed.
4. Program any changes of the system sensors and messages.
5. Program and connect the system for radio, email, phone, or other communication options as identified by the court and security.
6. Provide additional training on the installed equipment as necessary.
7. Control and account for tools in accordance with the existing Facilities Services *Tool Control Policy* as work is done throughout the facility, with increased attention in detention spaces.

Court

1. Provide access to vendor employees as necessary to perform the work.
2. Provide key contact information for scheduling work.
3. Identify locations for duress buttons and an appropriate location for the headend receiver device.

4. Identify which notification methods will be used.
5. Work with the vendor to properly identify the locations, naming convention, and appropriate messages to be communicated.
6. Provide network and/or telephone connectivity, if approved by court IT, along with IP addressing detail as required by the contractor.
7. Identify staff who need to be trained on the equipment and administrative access levels for users, and coordinate with the contractor for training.
8. Provide instructions and procedures to facilitate remote access to the system for maintenance and troubleshooting, if approved by court IT.
9. Identify who will sign the acceptance form on completion of the work.

Exclusions

- Excluded items include, but are not limited to, millwork, patching and painting, abatement of asbestos or lead-based paint, and cost of after-hours, weekend, or holiday escort, if required by the court.

- Additional exclusions may be included in specific scopes of work provided by the vendor.

Detention Control Systems

Detention Control Systems are complex and extremely expensive. Because of the significant cost of these systems, the number of detention control replacement/upgrade projects must be limited each fiscal year to allow sufficient funding for the other electronic security systems projects. Absent sufficient funding, detention control projects may need to be addressed through the Trial Court Facility Modification Advisory Committee process and funding.

Scope of work

1. Evaluate the existing detention control system based on current technology and potential security vulnerability to provide efficient and secure control of detainees.
2. Update any existing system hardware and software as needed.
3. Identify any integration between security components, including video, access control, intercom, and wireless duress alarm systems, and confirm the potential impact of changes to the detention control system with suggestions for mitigation.
4. Include replacing the detention control intercom system or components, if necessary, in detention control system upgrade projects.
5. Connect critical components to existing UPS systems, or provide UPS components as needed.

Components may include touchscreen panels, workstations, servers, programmable logic controller components, power supplies, intercom system components, cabling, UPS components, or any licensing required for a complete and functioning system.

Responsibilities

EPSCU

1. Coordinate meetings with court and Judicial Council contacts.
2. Provide information to the court and security on the capability of the system and the advantages of radio communication if the court and security providers are unfamiliar with the concept and application in a court environment.
3. Assist with coordination of ACM and lead-based paint testing between the court and testing vendor.
4. Include discussion of after-hours access and escorting during the project, if necessary.
5. Facilitate coordination of disposal of e-waste and other removed components.

Vendor

1. Conduct a kickoff meeting explaining the work process and how it may affect the court.
2. Coordinate with the court the scheduling of the work, and determine which areas, if any, will be affected by the project to minimize disruptions.
3. Clean up as work is completed in each area.
4. Control and account for tools in accordance with the existing Facilities Services *Tool Control Policy* as work is done throughout the facility, with increased attention in detention spaces.
5. Coordinate with IT and other court staff for access to space or network resources such as switch ports and IP addresses.
6. When ACM is present, observe proper Class III certification and practices as required.
7. Program individual or group user access levels to the system as instructed by the court.
8. Provide training on the installed equipment.

Court

1. Provide access to vendor employees as necessary to perform the work.
2. Provide key contact information for scheduling work.
3. Provide a staging location for materials and work area.
4. Work with the contractor to identify appropriate locations for door control panels and power supplies.
5. Provide network connectivity if approved by court IT, along with IP addressing detail as required by the contractor.

6. Identify staff who need to be trained on the equipment and administrative access levels for users, and coordinate with the contractor for training.
7. Identify who will sign the acceptance form on completion of the work.

Exclusions

- Excluded items include, but are not limited to, millwork, patching and painting, abatement of asbestos or lead-based paint, and the cost of after-hours, weekend, or holiday escort, if required by the court.
- Additional exclusions may be included in specific scopes of work provided by the vendor.

Resources

1. *Strategic Plan for the California Judicial Branch*
2. EPSCU's *Security Systems Design Criteria Guide*
3. Rule 10.61(a) of the California Rules of Court

Attachment A—Project Prioritization Scoring Sheet

County	
Facility Name	
FMID#	

Questions/Considerations	Possible Points	Score
Maintenance History		
0 Service Calls per Year	0	
1–4 Service Calls per Year	5	
5–10 Service Calls per Year	10	
10+ Service Calls per Year	15	
Age of Current System		
0–4 Years	0	
5–8 Years	5	
8–12 Years	10	
12+ Years	15	
Security Risk		
Low	1	
Medium	2	
High	3	
Recent Security Incidents (2 years)		
Yes	3	
No	0	
Deficiencies		
Yes	3	
No	0	
Recent Courtwide Projects (2 years)		
Yes	0	
No	3	
Upcoming Capital Projects (5 years)		
Yes	0	
No	3	

Magnitude of Project (cost)		
Less than 100K	5	
100K–250K	4	
250K–500K	3	
500K+	2	
Distance From Service Provider		
Within 1–2 Hours	0	
Within 2–3 Hours	2	
3–4 Hours	5	
4+ Hours	10	
Required Service Contract (third-party vendor)		
Yes	3	
No	0	
Deferred Project From Previous Fiscal Year		
Yes	5	
Total Score		

Note:
Additional factors to be considered, but not scored, are recommendations made during system evaluations or assessments and availability of funds.