www.courts.ca.gov/committee.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF ACTION BY EMAIL BETWEEN MEETINGS
OCTOBER 2, 2024

Email Proposal

At its August 12, 2024, meeting, this committee approved the proposed awards for the Language Access Signage and Technology (S&T) Grant Program, Cycle 6, Fiscal Year 2024–25. However, due to ongoing budget discussions, the committee considered revised recommended allocations prior to submission to the Judicial Council. These revisions reflected a 7.95% overall reduction in the judiciary's budget, with a recommendation to allocate additional funds if they become available. The revisions were highlighted in the materials provided and are listed below:

- $2.16M total S&T grant funding (updated from $2.35M) to reflect the 7.95% reductions;
- Highlighted paragraph on page 4: now has updated approval dates for committees; and
- Other updates are stylistic – changes to wording or provided clarification.

Notice

On September 30, 2024, a notice was posted advising that the Judicial Council Technology Committee was proposing to act by email on Wednesday, October 2, 2024, at 9:00 a.m., under California Rules of Court, rule 10.75(o)(1)(B).

Public Comment

Because the email recommendation concerned a subject that otherwise must be discussed in an open meeting, the Judicial Council Technology Committee invited public comment on the proposed branch technology priorities under rule 10.75(o)(2). The public comment period began at 12:00 p.m. on September 30, 2024, and ended at 9:00 a.m. October 2, 2024. No public comments were received.

Action Taken

After the public comment period ended, the Judicial Council Technology Committee members were asked to submit their votes by 9:00 a.m. on October 4, 2024, to approve the revised report and updated recommended allocations. The item passed with seven members approving the revisions and two abstaining.

Judicial Council of California
Technology Committee

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF OPEN MEETING

October 14, 2024
12:00 p.m. to 1:00 p.m.
Videoconference

Advisory Body Members Present:	Hon. Kyle S. Brodie, Chair; Hon. Maria D. Hernandez, Vice-Chair; Hon. C. Todd Bottke; Hon. Carol A. Corrigan; Ms. Rachel Hill; Mr. Charles Johnson; Mr. Darrel E. Parker
Advisory Body Members Absent:	Hon. Michelle Williams Court; Mr. Craig Peters
Others Present:	Hon. Sheila F. Hanson; Mr. John Yee; Mr. Juan Ambriz; and Judicial Council staff

OPEN MEETING

Call to Order and Roll Call

The chair called the meeting to order. Staff took roll call and made the opening announcements.

Approval of Minutes

The committee reviewed the draft minutes of the September 9, 2024 open meeting.

Action: The committee approved the minutes of the September 9, 2024 open meeting.

There were no written comments from members of the public received for this meeting.

DISCUSSION AND ACTION ITEMS (ITEMS 1–5)

Item 1

Chair Report (No Action – Information Only)

The committee received an update on activities and news from the Judicial Council, advisory bodies, courts, and/or other justice partners.

Item 2

Information Technology Advisory Committee (ITAC): Update and Report (No Action – Information Only)

The committee received an update and report on ITAC activities, including the activities of workstreams.

Item 3

Jury Management System Grant Program for the Fiscal Year 2024-25 (Action Requested)

The committee will consider the recommended allocations for the Jury Management System Grant program for fiscal year 2024-25. The budget for the Jury System Grant Program is funded by royalties from publishing jury instructions which are deposited in the Trial Court Improvement and Modernization Fund. These funds can only be used for jury-related technology projects. Funding allocations are proposed according to the objectives of the program, prioritization categories, other considerations, and funding metrics.

Action: The committee approved the recommended allocations for the Jury Management System Grant program for fiscal year 2024-25.

Item 4

Jury Management System Grant Program Revision for the Fiscal Year 2023-24 (Action Requested)

The committee will consider the recommended revision for the Jury Management System Grant program for the fiscal year 2023-24. The Superior Court of California, County of San Francisco is requesting approval to revise the scope of a project previously approved by the committee. The requested revision does not include any additional funding.

Action: The committee approved the revision for the Jury Management System Grant program for FY 2023-24 for the Superior Court of California, County of San Francisco.

Item 5

Judicial Branch Technology: Rules for Adoption of Technological and Data Security Standards (Action Requested)

Review draft invitation to comment on the proposal to revise California Rules of Court, rule 10.172 and adopt rule 10.405, which allow the Judicial Council to adopt standards for technological and data security for the courts. Consider approval to circulate proposal for public comment.

Action: This item was deferred to a future meeting.

ADJOURNMENT

There being no further business, the meeting was adjourned.

Approved by the advisory body on enter date.

Judicial Council *of* California

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

www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

W25-01

Title
Judicial Branch Technology: Rules for Adoption of Technology and Data Security Guidelines

Proposed Rules, Forms, Standards, or Statutes
Adopt Cal. Rules of Court, rule 10.405; amend Cal. Rules of Court, rule 10.172

Proposed by
Court Executives Advisory Committee
Darrel Parker, Chair
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Action Requested
Review and submit comments by January 6, 2025

Proposed Effective Date
July 1, 2025

Contact
Jenny Grantz, 415-865-4394
jenny.grantz@jud.ca.gov

Executive Summary and Origin

The Court Executives Advisory Committee and the Information Technology Advisory Committee propose amending one rule and adopting one rule to create a process for adopting and revising technology and data security guidelines for the courts and the Judicial Council. This proposal originated with the Joint Information Security Governance Subcommittee, which reviews and recommends guidelines, policies, and other security-related proposals for action by the Information Technology Advisory Committee and the Court Executives Advisory Committee.

Background

In 2023, the Court Executives Advisory Committee (CEAC) and the Information Technology Advisory Committee (ITAC) formed the Joint Information Security Governance Subcommittee (JISGS). JISGS develops cybersecurity and data protection initiatives on behalf of the judicial branch and reviews and makes recommendations on branchwide incident management, security

This proposal has not been approved by the Judicial Council and is not intended to represent the views of the council, its Rules Committee, or its Legislation Committee. It is circulated for comment purposes only.

training, and security policies. JISGS's goal is to give the Judicial Council confidence that information security policies have been adequately vetted and have branchwide support.

As a result of its work over the past year, JISGS believes that it would be beneficial for the Judicial Council to adopt guidelines for technology and data security that would apply to the courts and the council. These guidelines would help to ensure a minimum level of information security across the branch and would also enable the branch to apply information security best practices more effectively.

The Proposal

To create procedures for adopting and revising technology and data security guidelines for the courts and the council, the committees propose amending one rule and adopting one rule.

Rule 10.172

Existing rule 10.172 requires each superior court to develop a court security plan that addresses numerous subject areas. The committees propose moving the computer and data security subject area to new rule 10.405. To do so, the committees propose:

- Revising subdivision (a) to refer to a "court security plan that applies to each court facility in the county" instead of a "countywide court security plan" to clarify that rule 10.172 addresses security in court facilities;

- Revising subdivision (b)(1) to remove subpart (V), "computer and data security," because that topic will be covered by new rule 10.405; and

- Adding a second sentence to the Advisory Committee Comment to inform readers that computer and data security are now covered by rule 10.405 instead of rule 10.172.

Rule 10.405

The committees propose adopting new rule 10.405 to create the process for adopting and revising technology and data security guidelines for the courts and the Judicial Council.

Subdivision (a) provides the rule's purpose, which is to create procedures for the adoption and maintenance of judicial branch guidelines for technology and data security.

Subdivision (b) describes process for adopting and revising the guidelines. The committees decided to make ITAC responsible for developing the guidelines and making recommendations to the Judicial Council because ITAC's membership includes judicial officers, court executives, court technologists, and other subject matter experts, and ITAC has extensive experience developing proposals to address technology issues affecting the courts.

Subdivision (b) also creates a 30-day period during which the courts can comment on proposed new or revised guidelines before ITAC makes a recommendation to the Judicial Council. The committees' goal is to ensure that all courts are given sufficient notice and opportunity to

DRAFT

provide input on the guidelines. The language in subdivision (b)(2) was modeled on rule 10.804(b)(1), which contains a similar comment process.[1] The Technology Committee has the authority to approve nonsubstantive technical changes or corrections to the guidelines without Judicial Council approval and without the 30-day comment period. This provision is similar to provisions in other rules that allow for technical changes and corrections without council approval.[2]

Subdivision (c) clarifies that any guidelines adopted under rule 10.405 apply to the Supreme Court, the Courts of Appeal, the superior courts, and the Judicial Council.

Subdivision (d) clarifies that for security reasons, any guidelines adopted under rule 10.405 are exempt from public disclosure under rule 10.500.[3] This exemption is necessary because the need to protect judicial branch security by limiting access to the guidelines outweighs the public interest in disclosure of judicial administrative records. Disclosure of records relating to the guidelines, which may include specific methods used to secure judicial branch technology and data, would compromise the ability of the courts and the Judicial Council to protect their systems and data, as well as court users' personal information.

Alternatives Considered

The committees considered taking no action but ultimately determined that the proposal was warranted because creating technology and data security guidelines could provide tremendous benefits to the courts and the Judicial Council.

Fiscal and Operational Impacts

The guidelines adopted under proposed rule 10.405 might require courts to implement or change their policies or procedures, which might require training for judicial officers and court staff. Courts might also need to procure equipment or services to meet the guidelines adopted under rule 10.405.

---

[1] Rule 10.804(b)(1) reads: "Before making any substantive amendments to the *Trial Court Financial Policies and Procedures Manual*, the Judicial Council must make the amendments available to the superior courts, the California Department of Finance, and the State Controller's Office for 30 days for comment."

[2] For example, rule 10.804(b)(2) allows the Administrative Director to make technical changes and corrections to the *Trial Court Financial Policies and Procedures Manual*. Similarly, rule 10.22(d)(2) allows the Rules Committee to recommend "nonsubstantive technical change[s] or correction[s]" to the California Rules of Court and Judicial Council forms without circulating the proposed changes for public comment.

[3] Rule 10.500(f)(6) exempts from disclosure any "[r]ecords whose disclosure would compromise the security of a judicial branch entity or the safety of judicial branch personnel, including but not limited to, court security plans, and security surveys, investigations, procedures, and assessments." Rule 10.500(f)(6) and proposed rule 10.405(d) are consistent with the California Public Records Act's exemption for information security records. (Gov. Code, § 7929.210.)

Request for Specific Comments

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

- Does the proposal appropriately address the stated purpose?

The advisory committees also seek comments from *courts* on the following cost and implementation matters:

- Would the proposal provide cost savings? If so, please quantify.
- What would the implementation requirements be for courts—for example, training staff (please identify position and expected hours of training), revising processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems?
- Would three months from Judicial Council approval of this proposal until its effective date provide sufficient time for implementation?
- How well would this proposal work in courts of different sizes?
- Does the proposal appropriately address the different characteristics of the Supreme Court, the Courts of Appeal, the superior courts, and the Judicial Council?

Attachments

1. Cal. Rules of Court, rules 10.172 and 10.405, at pages 5–9

DRAFT

Rule 10.172 of the California Rules of Court would be amended, effective July 1, 2025, to read:

Title 10. Judicial Administration Rules

Division 2. Administration of the Judicial Branch

Chapter 2. Court Security

Rule 10.172. Court security plans

(a) Responsibility

The presiding judge and the sheriff or marshal are responsible for developing an annual or multiyear comprehensive, ~~countywide~~ court security plan that applies to each court facility in the county.

(b) Scope of security plan

(1) Each court security plan must, at a minimum, address the following general security subject areas:

(A) Composition and role of court security committees;

(B) Composition and role of executive team;

(C) Incident command system;

(D) Self-assessments and audits of court security;

(E) Mail handling security;

(F) Identification cards and access control;

(G) Courthouse landscaping security plan;

(H) Parking plan security;

(I) Interior and exterior lighting plan security;

(J) Intrusion and panic alarm systems;

(K) Fire detection and equipment;

Rule 10.172 of the California Rules of Court would be amended, effective July 1, 2025, to read:

(L) Emergency and auxiliary power;

(M) Use of private security contractors;

(N) Use of court attendants and employees;

(O) Administrative/clerk's office security;

(P) Jury personnel and jury room security;

(Q) Security for public demonstrations;

(R) Vital records storage security;

(S) Evacuation planning;

(T) Security for after-hours operations;

(U) Custodial services;

~~(V) Computer and data security;~~

(V~~W~~) Workplace violence prevention; and

(W~~X~~) Public access to court proceedings.

(2) Each court security plan must, at a minimum, address the following law enforcement subject areas:

(A) Security personnel and staffing;

(B) Perimeter and entry screening;

(C) Prisoner and inmate transport;

(D) Holding cells;

(E) Interior and public waiting area security;

(F) Courtroom security;

(G) Jury trial procedures;

Rule 10.172 of the California Rules of Court would be amended, effective July 1, 2025, to read:

(H) High-profile and high-risk trial security;

(I) Judicial protection;

(J) Incident reporting and recording;

(K) Security personnel training;

(L) Courthouse security communication;

(M) Hostage, escape, lockdown, and active shooter procedures;

(N) Firearms policies and procedures; and

(O) Restraint of defendants.

(3) Each court security plan should address additional security issues as needed.

(c) Court security assessment and assessment report

At least once every two years, the presiding judge and the sheriff or marshal are responsible for conducting an assessment of security with respect to all court operations. The assessment must include a comprehensive review of the court's physical security profile and security protocols and procedures. The assessment should identify security weaknesses, resource deficiencies, compliance with the court security plan, and any need for changes to the court security plan. The assessment must be summarized in a written assessment report.

(d) Submission of court a plan to the Judicial Council

On or before November 1, 2009, each superior court must submit a court security plan to the Judicial Council. On or before February 1, 2011, and each succeeding February 1, each superior court must give notice to the Judicial Council whether it has made any changes to the court security plan and, if so, identify each change made and provide copies of the current court security plan and current assessment report. In preparing any submission, a court may request technical assistance from Judicial Council staff.

Rule 10.172 of the California Rules of Court would be amended, effective July 1, 2025, to read:

(e) Plan review process

Judicial Council staff will evaluate for completeness submissions identified in (d). Annually, the submissions and evaluations will be provided to the Court Security Advisory Committee. Any submissions determined by the advisory committee to be incomplete or deficient must be returned to the submitting court for correction and completion.

(f) Delegation

The presiding judge may delegate any of the specific duties listed in this rule to another judge or, if the duty does not require the exercise of judicial authority, to the court executive officer or other court employee. The presiding judge remains responsible for all duties listed in this rule even if he or she has delegated particular tasks to someone else.

Advisory Committee Comment

This rule is adopted to comply with the mandate in Government Code section 69925, which requires the Judicial Council to provide for the areas to be addressed in a court security plan and to establish a process for the review of such plans.

Former subdivision (b)(1)(V), on computer and data security, is now addressed in rule 10.405, on judicial branch technology and data security standards.

Rule 10.405 of the California Rules of Court would be adopted, effective July 1, 2025, to read:

Title 10. Judicial Administration Rules

Division 2. Administration of the Judicial Branch

Chapter 6. Court Technology, Information, and Automation

Rule 10.405. Judicial branch technology and data security guidelines

(a) Purpose

This rule creates procedures for the adoption and maintenance of judicial branch guidelines for technology and data security.

(b) Adoption and maintenance of guidelines

(1) The Information Technology Advisory Committee is responsible for making recommendations to the Judicial Council regarding guidelines for technology and data security.

(2) Before recommending to the Judicial Council the adoption of any new guidelines or substantive amendments to the guidelines, the Information Technology Advisory Committee must make the proposed guidelines available to the entities listed in subdivision (c) for 30 days for comment.

(3) The Judicial Council delegates to the Technology Committee the authority to make nonsubstantive technical changes or corrections to the guidelines. Upon the recommendation of the Information Technology Advisory Committee, the Technology Committee may approve nonsubstantive technical changes or corrections to the guidelines without the comment period required in subdivision (b)(2) and without approval by the Judicial Council.

(c) Application of guidelines

The guidelines apply to the Supreme Court, the Courts of Appeal, the superior courts, and the Judicial Council.

(d) Disclosure of guidelines

The guidelines are exempt from public disclosure consistent with the provisions of rule 10.500 that exempt records whose disclosure would compromise the security of a judicial branch entity.