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 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 (CEAC) and the Information Technology Advisory Committee (ITAC) 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 security-related guidelines, policies, and other proposals for action by ITAC and CEAC.

Background

In 2023, the Court Executives Advisory Committee and the Information Technology Advisory Committee 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 training, and security policies. JISGS's goal is to adequately vet and secure branchwide support for information security policies.

As a result of its work over the past year, JISGS concluded 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 establish 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:

- Amending subdivision (a) to clarify its meaning by referring to a "court security plan that applies to each court facility in the county" instead of a "countywide court security plan";
- Amending 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 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.

The committees ask for specific comments on whether it is appropriate to amend rule 10.172(a). The proposed amendments to subdivision (a) are intended to be clarifying, not to change its meaning or scope.

Rule 10.405

The committees propose adopting new rule 10.405 to establish 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 set forth procedures for the adoption and maintenance of judicial branch guidelines for technology and data security.

Subdivision (b) describes the process for adopting and revising the guidelines. The committees propose that ITAC be 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. Additionally, ITAC has extensive experience developing proposals to address technology issues affecting the courts.

Subdivision (b) also proposes 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

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 proposed rule provides the Technology Committee with 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) provides 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) provides 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 of the strong need to protect judicial branch security by limiting access to the guidelines, which clearly outweighs the public interest in disclosure of these records. Disclosure of the guidelines and any 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 would provide significant 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*.

[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?
- Is it appropriate to amend subdivision (a) of rule 10.172 to clarify its meaning, or is the existing wording of that subdivision preferable?

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 two 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

Rule 10.405 of the California Rules of Court would be adopted and rule 10.172 would be amended, effective July 1, 2025, to read:

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;

(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;~~

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

~~(X)~~ (W) 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;

(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.

(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.

Computer and data security, formerly covered by subdivision (b)(1)(V), is now addressed in rule 10.405, on judicial branch technology and data security standards.

Rule 10.405. Judicial branch technology and data security guidelines

(a) Purpose

This rule sets forth 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 for technology and data security apply to the Supreme Court, the Courts of Appeal, the superior courts, and the Judicial Council.

(d) Disclosure of guidelines

The guidelines for technology and data security 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.