Judicial Council *of* California

455 Golden Gate Avenue · San Francisco, California 94102-3688
www.courts.ca.gov

REPORT TO THE JUDICIAL COUNCIL

Item No.: 25-073
For business meeting on April 25, 2025

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

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

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

Report Type
Action Required

Effective Date
July 1, 2025

Date of Report
April 8, 2025

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

Executive Summary

The Court Executives Advisory Committee (CEAC) and the Information Technology Advisory Committee (ITAC) recommend adopting one rule and amending 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.

Recommendation

The Court Executives Advisory Committee and the Information Technology Advisory Committee recommend that the Judicial Council, effective July 1, 2025:

1. Adopt California Rules of Court, rule 10.405 to create a process for adopting and revising technology and data security guidelines for the courts and the Judicial Council; and

2. Amend California Rules of Court, rule 10.172 to reflect the adoption of rule 10.405.

The proposed new rule and amended rule are attached at pages 6–10.

Relevant Previous Council Action

The Judicial Council adopted rule 10.172 effective January 1, 2009, to implement Government Code section 69925, which requires each superior court to develop a court security plan and requires the Judicial Council to determine which subject areas must be addressed in those plans.

The council last amended rule 10.172 effective January 1, 2016, to remove references to the Administrative Office of the Courts.

Analysis/Rationale

In 2023, CEAC and 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 training, and security policies. JISGS's goal is to 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 a process for developing and approving branchwide guidelines for technology and data security. The purpose of the guidelines will be to ensure a minimum level of information security across the branch and enable the branch to apply information security best practices more effectively. The proposed procedures for adopting the guidelines will give courts an opportunity to provide feedback while the guidelines are being developed, help ITAC identify potential implementation issues, and ensure that the guidelines will work for courts of all sizes and at all levels of information security experience and infrastructure.

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

Rule 10.405

The committees recommend 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 recommend that ITAC develop the guidelines and make 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 includes 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 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 presumptively 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.

[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.)

Rule 10.172

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

- 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.[4]

Before this proposal was circulated for comment, it was reviewed by the Court Security Advisory Committee, which raised no objection to these proposed revisions to rule 10.172. A predecessor of the Court Security Advisory Committee originally recommended adoption of the rule.

The version of rule 10.172 that circulated for public comment included an amendment to subdivision (a) that changed "countywide court security plan" to "court security plan that applies to each court facility in the county." The committees proposed this amendment to clarify the rule's meaning and did not intend to change the scope of the rule. The committees ultimately decided not to make this amendment because it was unclear whether the amendment improved the rule's clarity and because it could have created confusion about whether the rule's scope had been changed.

Policy implications

This proposal will create procedures for adopting guidelines for technology and data security for the courts and the Judicial Council. These guidelines will benefit the branch by ensuring a minimum level of information security across the branch and enabling the branch to apply information security best practices more effectively. The procedures in rule 10.405 will ensure that the guidelines are developed with the input of courts and will help ITAC develop guidelines that minimize implementation issues and address the needs of all courts.

This proposal is, therefore, consistent with the *Strategic Plan for California's Judicial Branch*, specifically the goals of Modernization of Management and Administration (Goal III) and Branchwide Infrastructure for Service Excellence (Goal VI).

Comments

This proposal was circulated for public comment from December 5, 2024, to January 6, 2025, as part of the regular winter invitation-to-comment cycle. One comment was received on the proposal, from the Superior Court of Los Angeles County. The commenter agreed with the

[4] The committees also recommend correcting a typographical error in the heading of rule 10.172(d).

proposal if modified. A chart with the full text of the comment received and the committees' responses is attached at pages 11–12.

The commenter suggested that when guidelines are adopted under rule 10.405, general guidelines should be crafted to address minimum, entry-level requirements to ensure that the guidelines work for courts of all sizes. The commenter also noted that when guidelines are adopted, their substance and complexity will determine how quickly courts can implement them.

Additionally, the commenter suggested amending rule 10.405 to include a control, audit, or review mechanism to ensure that courts adhere to guidelines adopted under the rule. The committees agree that such a mechanism could be beneficial but have not amended the rule to include one because those amendments would go beyond the scope of the current proposal and would require public comment. The committees will consider this suggestion as time and resources permit.

Alternatives considered

The committees considered the alternative of taking no action but ultimately determined that the proposal was warranted because creating a process for developing and approving technology and data security guidelines would provide significant benefits to the public, courts, and the Judicial Council.

In addition, as discussed above, the committees considered several alternatives when drafting and revising the rules, including alternatives suggested by the commenter.

Fiscal and Operational Impacts

The guidelines adopted under 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.

Attachments and Links

1. Cal. Rules of Court, rules 10.172 and 10.405, at pages 6–10
2. Chart of comments, at pages 11–12

Rule 10.405 of the California Rules of Court is adopted and rule 10.172 is 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.

(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~~ security 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 guidelines.

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 (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 (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.

W25-01

Judicial Branch Technology: Rules for Adoption of Technology and Data Security Guidelines (Adopt Cal. Rules of Court, rule 10.405; amend rule 10.172)

All comments are verbatim unless indicated by an asterisk (*).

	Commenter	Position	Comment	Committee Response
1.	Superior Court of California, County of Los Angeles by Robert Oftring, Director, Communications and Legislative Affairs	A	The following comments are representative of the Superior Court of California, County of Los Angeles, and do not represent or promote the viewpoint of any particular judicial officer or employee.	No response required.
			In response to the Judicial Council of California's proposal titled "ITC W25-01: Judicial Branch Technology: Rules for Adoption of Technology and Data Security Guidelines," the Superior Court of California, County of Los Angeles (Court), concurs that the proposal addresses its intended purpose.	The committees appreciate the response.
			The Court agrees that it is appropriate to amend subdivision (a) of rule 10.172 to clarify its meaning.	The committees appreciate the response.
			The Court does not believe the proposal would provide cost savings. The JCC would need to also provide funding for initiatives and guidelines related to this proposal.	The committees appreciate the response.
			To implement the proposal, the Court would need to revise policies, update processes and procedures, and train staff. It would also need to implement new tools to support the guidelines.	The committees appreciate the response.
			It is unclear if two months from Judicial Council approval would be sufficient time to implement. It would depend on the guidelines and how complex the implementation would be.	The committees appreciate the response. The committees note that the two-month timeframe discussed in the request for specific comment is referring to the time to implement the new and

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated

	Commenter	Position	Comment	Committee Response
			A longer time period should be considered.	amended rules in this proposal, rather than the time to implement any guidelines adopted under rule 10.405.
			General guidelines should be crafted to address minimum requirements and define those as entry level. If that is done, then it should work for courts of all sizes.	The committees appreciate the response.
			For general comments, the current rule lacks a control, audit, or review mechanism to ensure that courts adhere to its provisions. To address this, it would be beneficial to establish a framework of good-better-best guideline rates, providing courts with a clear spectrum of options to decide where they align within the guidelines. Additionally, adopting a risk-based approach would allow courts to assess the specific risks applicable to them, evaluate the severity of those risks, and determine an appropriate level of mitigation based on their unique circumstances.	Amending rule 10.405 to include a control, audit, or review mechanism would require public comment and therefore cannot be included in this proposal, but the committees will consider this suggestion as time and resources permit.