Tactical Plan for Technology 2025-26

Hon. Sheila Hanson, *Chair, Information Technology Advisory Committee*
Brian Cotta, *CEO, Fifth District Court of Appeal; Tactical Plan Workstream Member*

January 21, 2025

What’s changed?

- **Introduction**
- Additions based on **public comments**

Requested Action

Recommend **2025 – 2026 Tactical Plan for Technology** for submission to the Technology Committee.

Thank you!

Rule Proposal: Branchwide Technology and Data Security Guidelines

Hon. Tara M. Desautels,
Associate Justice, Court of Appeal, First Appellate District

Meeting of the Information Technology Advisory Committee
January 21, 2025

Overview

- Public comment on the rule proposal closed on January 6; proposal is ready to go to the Judicial Council for approval
  - The proposal received one public comment
  - JISGS made one change to the proposal for rule 10.172 after circulating for comment
- Action requested: Approve Judicial Council report
- Next steps:
  - Approval by CEAC (Feb. 7), Technology Committee (Feb. 10), and Rules Committee (Mar. 13) (already approved by JISGS and RPS, Jan. 16)
  - Judicial Council meeting (April 25)
  - Effective date, if approved by council: July 1, 2025

Rule 10.405

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.

Public Comment

- One public comment received: Superior Court of Los Angeles County
- Comment: Rule 10.405 should be amended to include a control or audit mechanism to ensure courts follow the guidelines.
    - JISGS will consider how to address monitoring/verification as it develops guidelines.
    - But this amendment would require public comment and cannot be made now.
- Comment: When adopting guidelines under rule 10.405, ensure the scope and timeline will work for all court sizes.
    - JISGS will keep these issues in mind as it develops guidelines.

Public Comment

Complete text of the relevant portions of the comment and the proposed responses:

Comment	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. A longer time period should be considered.	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 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.

Rule 10.172

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:

* * *

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

* * *

Advisory Committee Comment

* * *

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.

Change to Rule 10.172(a)

Rule 10.172(a):

Proposed in Invitation to Comment	Recommended in Judicial Council Report
The presiding judge and the sheriff or marshal are responsible for developing an annual or multiyear comprehensive, court security plan that applies to each court facility in the county.	The presiding judge and the sheriff or marshal are responsible for developing an annual or multiyear comprehensive, countywide court security plan. *(identical to the currently effective version of the rule)*

Change to Rule 10.172(a)

- Proposal included amendments to subdivision (a) of rule 10.172
  - Was: “countywide court security plan”
  - Proposed: “court security plan that applies to each court facility in the county”
- At subsequent JISGS and RPS meetings, members were concerned this amendment may interfere with existing MOUs
- JISGS agreed to withdraw the amendment to (a). JISGS and RPS members approved the proposed amendments to (b) and the Advisory Committee Comment

Questions or comments?