Rule Proposal: Branchwide Technological and Data Security Standards

Hon. Tara M. Desautels,
Associate Justice, Court of Appeal, First Appellate District
Jenny Grantz,
Attorney, Legal Services

Meeting of the Information Technology Advisory Committee
September 25, 2024

Overview

- Joint Information Security Governance Subcommittee (JISGS) proposes rule amendments to allow the Judicial Council to adopt branchwide standards for technological and data security
- Action requested: Approve draft invitation to comment
- Next steps:
  - Approval by Technology Committee, CEAC, Rules Committee
  - Circulate for public comment from December 6, 2024 to January 6, 2025

Rule Proposal Background

- Goal is to create branchwide technological and data security standards in order to:
  - Ensure minimum level of information security across the branch
  - Help the branch apply information security best practices
- Today we present our first proposed rule changes:
  - Clarifies the division of responsibility for physical and technological security;
  - Creates a process for developing, adopting, and revising the technological security standards; and
  - Enables standards to be developed after rules adoption.

Amendments to Rule 10.172

- Rule 10.172 requires each superior court to develop a court security plan that addresses numerous subject areas
- JISGS proposes removing technological security from this rule and moving it to a new rule of court:
  - Delete “computer and data security” from the list of topics included in a court security plan
  - Add a sentence to the Advisory Committee Comment to directing readers to rule 10.405 for computer and data security
  - Revise subdivision (a) to clarify that rule 10.172 addresses security in court facilities

Amendments to 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 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:

* * *

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

* * *

Advisory Committee Comment

* * *

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.

New Rule 10.405

- Creates the procedures for adopting and revising branchwide technological and data security standards
- Key provisions:
  - Standards will be developed by ITAC (can be delegated to JISGS); approved by Technology Committee and Judicial Council
  - 30-day period for courts to comment on all substantive amendments
  - Standards apply to all courts and the Judicial Council
  - Standards are exempt from public disclosure under rule 10.500

New Rule 10.405

Rule 10.405. Judicial branch technology and data security standards

(a) Adoption and maintenance of standards

The Judicial Council may adopt and maintain judicial branch standards for technological and data security. The Information Technology Advisory Committee will be responsible for developing the standards, making any revisions, and making recommendations to the Judicial Council.

(b) Revisions to the standards

(1) Before making any substantive amendments to the standards, the Information Technology Advisory Committee must make the amendments available to the entities listed in subdivision (c) for 30 days for comment.

(2) Upon the recommendation of the Information Technology Advisory Committee, the Technology Committee may approve nonsubstantive technical changes or corrections without the comment period required in subdivision (b)(1) and without approval by the Judicial Council.

(c) Application of standards

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

(d) Disclosure of standards

The standards 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.

Questions or comments?