



## JUDICIAL COUNCIL OF CALIFORNIA

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

[www.courts.ca.gov](http://www.courts.ca.gov)

---

# REPORT TO THE JUDICIAL COUNCIL

For business meeting on February 19, 2015

---

**Title**

Judicial Branch Administration: Fiscal Year  
2015–2016 Budget Change Proposal to  
Strengthen Information System Security and  
Data Reliability

**Agenda Item Type**

Action Required

**Effective Date**

February 19, 2015

**Rules, Forms, Standards, or Statutes Affected**

None

**Date of Report**

February 18, 2015

**Recommended by**

Judicial Council Technology Committee  
Hon. James E. Herman, Chair  
Judicial Council Staff  
Curt Soderlund, Chief Administrative Officer  
Zlatko Theodorovic, Director  
Finance

**Contact**

Curt Soderlund, 916-263-5512  
[curt.soderlund@jud.ca.gov](mailto:curt.soderlund@jud.ca.gov)

---

### Executive Summary

In August 2014, the Judicial Council approved a conceptual outline for funding the additional work needed to fully implement an information security program and resolve California State Auditor recommendations. In alignment with this approved concept, Judicial Council staff recommends and the Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch supports augmenting the General Fund in fiscal year 2015–2016 to implement recommendations from the California State Auditor. The recommended augmentation—of \$2.4 million, with an ongoing commitment of an additional \$1.1 million in subsequent years—would allow the Judicial Council to comply with the State Auditor’s recommendations in separate audit reports and confidential management letters issued on judicial branch procurement in 2013 and on a statewide review of data reliability in 2014. This proposed funding augmentation includes support for three full-time equivalent positions, which are necessary

because existing staff levels cannot support these additional duties. These positions would serve to safeguard Judicial Council information systems while also serving the broader data assurance objectives for California's state government in biennial reporting by the State Auditor since 2008.

## **Recommendation**

Judicial Council staff—with oversight from the chairs of the Judicial Council Technology Committee (JCTC), Trial Court Presiding Judges Advisory Committee (TCPJAC), and Court Executives Advisory Committee (CEAC)—recommend that the Judicial Council approve the submission of a budget change proposal to the State Department of Finance requesting a one-time augmentation of \$2.4 million in fiscal year 2015–2016 and an additional \$1.1 million in subsequent fiscal years. The purpose of this augmentation is to implement recommendations from the California State Auditor intended to strengthen security controls and assure the reliability of judicial branch data. The funding requested will be used to achieve the following deliverables and objectives:

### **1. Audit and Accountability**

- Deliverable: Implementation of user-access auditing tools that enable the courts to locally collect and monitor server log data and report on user account changes
- Budget: \$615,000 one time and \$47,000 ongoing
- Objective: A centrally funded auditing program that provides licensing for the courts to use the same auditing tools implemented within the Judicial Council, without diverting court funding from other priorities

### **2. Risk Assessment**

- Deliverable: Establishment of periodic organizational risk assessments of Judicial Council information systems
- Budget: \$210,000 one time and \$208,000 ongoing
- Objective: Ongoing risk assessments to determine risk and magnitude of harm associated with unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support their operations and assets

### **3. Contingency Planning**

- Deliverable: Implementation of a disaster recovery program to guard against inadvertent disruptions of Judicial Council information systems and data loss
- Budget: \$889,000 one time and \$512,000 ongoing
- Objective: A disaster recovery program to ensure service continuity by addressing potential disruptions in information technology systems, from minor interruptions, such as temporary power failures, to major disasters, such as fires, natural disasters, and terrorism

4. Security Program Management
  - Deliverable: Implementation of a formalized security program for Judicial Council information systems
  - Budget: \$365,000 one time and \$345,000 ongoing
  - Objective: Improvements in the security program for Judicial Council information systems to implement and enforce best practices to avoid risk of compromising data and data loss
  
5. Media Protection
  - Deliverable: Complete preparations for the implementation of a data classification program within the Judicial Council
  - Budget: \$325,000 one time
  - Objective: A properly architected data classification program to ensure that data is stored, labeled, and safeguarded appropriately according to its classification and that the appropriate security measures are followed to preserve the integrity, availability, and required level of confidentiality of the council's information resources
  
6. Staff Support (3.0 full-time equivalent [FTE] positions included in the figures above to perform the following functions)
  - A disaster recovery program (referenced above in item 3, Contingency Planning) for a workload increase that will require one additional position for a full-time Business System Analyst to administer the program
  - A security program (referenced above in item 4, Security Program Management) for a workload increase that will require the addition of 1.0 FTE Supervising Analyst B position and 1.0 FTE Business Systems Analyst position for developing and overseeing a security operation, enforcing compliance standards, and working with external agencies to communicate threats and vulnerabilities

### **Previous Council Action**

In 2013, the California State Auditor issued an audit report and confidential management letters advising that the Judicial Council needed to make immediate improvements in the controls applied to secure the council's information systems and, in 2014, that although the Judicial Council had made strides internally to follow industry-standard best practices, the same capabilities, policies, and procedures implemented by the council needed to be implemented for the courts. Weaknesses cited included the need for periodic risk assessments to safeguard information systems from disruption and data loss.

Upon receipt of the auditor's recommendations, an oversight committee of the JCTC, TCPJAC, and CEAC chairs was established to guide the response. With the committee's oversight, the Judicial Council's Information Technology office implemented a framework of information systems controls and conducted a gap analysis within the Judicial Council that identified necessary improvements that cannot be addressed without additional staff and resources.

In February 2013, the Chief Justice authorized the creation of the Technology Planning Task Force. The task force was charged with working collaboratively to define judicial branch technology governance in terms of statewide versus local decisionmaking, to develop for technology across all court levels a strategic plan that provides a vision and direction for technology within the branch, and to develop recommendations for a stable, long-term funding source for supporting branch technology, as well as a delineation of technology funding sources.

In January 2014, the Judicial Council approved the [concept of the court technology governance and strategic plan](#), prepared by the Technology Planning Task Force, based on the information provided in the executive summary for the governance and funding model and plans.

In August 2014, the Judicial Council approved the [Court Technology Governance and Strategic Plan](#), which includes a Governance and Funding Model, Strategic Plan, and Tactical Plan. The chair of the JCTC stated that the plan would return to the council with updates related to language access.

Also, in August 2014, the Judicial Council approved a conceptual outline for funding the additional work needed to fully implement an information security program and resolve the California State Auditor recommendations. The conceptual proposal for a funding augmentation, however, did not provide specific cost details; the total amount was left to be determined. This proposal is being brought to the council for review and approval now that the financial and personnel commitments to accomplish the work have been identified and the level-of-effort calculations are available in greater detail.

In October 2014, the Judicial Council approved the [updated Court Technology Governance and Strategic Plan](#). Goal 2 (Optimize Branch Resources) and Goal 3 (Optimize Infrastructure) of the strategic plan are addressed by this budget change proposal (BCP). The BCP addresses two initiatives of the Tactical Plan for Technology: Court Information Systems Security Policy Framework and Court Disaster Recovery Framework and Pilot.

On February 4, 2015, the council's Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch reviewed the details of this funding augmentation and approved submitting the request to the Department of Finance for fiscal year 2015–2016.

### **Rationale for Recommendation**

The recommended funding augmentation of \$2.4 million in fiscal year 2015–2016 and \$1.1 million ongoing in subsequent years is needed to address weaknesses in the Judicial Council's existing information technology infrastructure that, if unaddressed, could compromise the security of branch data. Lack of sufficient funding to take corrective measures would leave the Judicial Council and the courts out of compliance with the State Auditor's directives to strengthen information security controls. These directives are part of a wider-reaching focus of the State Auditor to assess data reliability within the State's information technology systems.

Deficiencies identified by the auditor are reported to the Governor, legislative leaders, and the public.

Although the Judicial Council's Information Technology office has implemented some of the controls necessary for auditing user access within Judicial Council information systems, the work is incomplete. Additional resources are necessary to implement these same capabilities within the courts. Furthermore, in the analysis of the corrective measures needed to achieve the recommended level of data security, staff have identified work that remains in each of five key areas specified by the National Institute of Standards and Technology, an industry source on best practices for developing or enhancing an information security program. These five areas are considered basic components of a program to protect the integrity, availability, and confidentiality of agency data and safeguard information assets and resources and are part of the recommendation of this report to the council:

1. Audit and Accountability
2. Risk Assessment
3. Contingency Planning
4. Security Program Management
5. Media Protection

As referenced in the recommendation above, work which will require additional funding and resources, remains to be accomplished in each of these areas to fully implement a credible information security program for the Judicial Council and the trial courts.

### **Comments, Alternatives Considered, and Policy Implications**

As stated in the August 2014 report to the Judicial Council in which the conceptual outline for this funding augmentation was first proposed, the Judicial Council has statutory authority to approve budget requests on behalf of the Supreme Court, Courts of Appeal, Judicial Council, and Judicial Branch Facilities Program. Once the specific financial details of the proposal became known, Judicial Council staff submitted the proposal to the Advisory Committee on Financial Accountability and Efficiency for the Judicial Branch for review, in accordance with the council's fiscal oversight process. The committee reviewed the merits and the implications of this proposal and approved it.

The alternative to approving this proposal would be to forego requesting the funds needed to fully implement an information security program that meets industry standards for information technology and addresses the California State Auditor's recommendations. This course of action, however, would leave the Judicial Council's information systems vulnerable to an unacceptable level of risk, according to the State Auditor, and would fail to protect the information assets of the courts and the branch at a level expected for council oversight.

## **Implementation Requirements, Costs, and Operational Impacts**

Implementation requirements, costs, and operational impacts are detailed in the recommendation section above.

## **Relevant Strategic Plan Goals and Operational Plan Objectives**

This funding proposal, if approved and implemented, will address the strategic plan goals of Access, Fairness, and Diversity (Goal I), Modernization of Management and Administration (Goal III), and Quality of Justice and Service to the Public (Goal IV). The Judicial Council approved the Court Technology Governance and Strategic Plan, which includes the strategic and tactical plans for technology.

## **Attachments and Links**

1. Attachment A: [California State Auditor Report on Judicial Branch Procurement, Report 2013-302 and 2013-303](#)
2. Attachment B: [California State Auditor Report on Data Reliability, Report 2014-401](#)
3. Attachment C: [Budget: Fiscal Year 2015–2016 Budget Requests for the Supreme Court, Courts of Appeal, Judicial Council, and Judicial Branch Facilities Program](#)