A&E Committee Meeting
Implementation of Information Systems Control Enhancements
FY 2015-16 BCP

FY 15-16 BCP Program Background and Staffing Status

The FY 2015-16 BCP proposal for the implementation of information systems control enhancements requests $2.4 million (initial) and $1.1 million (ongoing) to implement recommendations from the California State Auditor that are related to strengthening security controls and assuring the reliability of Judicial Branch data. This includes the proposed addition of three staff members in the areas of security and disaster recovery. The State Auditor's report underscores the need for resources in these areas, however due to staff reductions and a hiring freeze over the last six fiscal years, the Information Technology Office has been unable to recruit and hire for these positions.

Current Year Conditions and Risks

Upon receipt of the auditor's findings and recommendations from the California State Auditors 2013 Judicial Branch Procurement Audit, the Chief Justice established a task force consisting of the chairs of the Judicial Council Technology Committee (JCTC), Trial Court Presiding Judges Advisory Committee (TCPJAC), and the Court Executive Advisory Committee (CEAC). Under their oversight, the Judicial Council Technology Office has worked to comply with the auditor's recommendations. These efforts have included the adoption of a framework of information systems controls, and a gap analysis to identify areas where additional focus was needed that could not be addressed with existing staff and resources. Five key areas specified by National Institute of Standards and Technology (NIST) standards have been identified as requiring additional funding and resources to fully implement.

Area 1. Audit and Accountability (NIST Control Set AU): While the Judicial Council has implemented the tools required to provide adequate auditing capabilities for transactions related to user access, these same capabilities must still be implemented within the trial courts.

- Background: This set of controls specifies the ability to (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information systems users can be uniquely traced to those users so they can be held accountable for their actions. While system and event logging capabilities have and continue to be in place, specialized tools are required to facilitate the aggregation and extended retention of those logs, and to facilitate the presentation of this data in a more useful and efficient manner.

Area 2. Risk Assessment (NIST Control Set RA): The Judicial Council security framework follows NIST standards that organizations must perform periodic information technology risk assessments. For these assessments to be objective, however, they should be performed by external qualified parties. As a result, these assessments will result in costs that are unable to be covered within the Judicial Council's existing budget.

- Background: This set of controls specifies the need to conduct periodic assessments of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, and other organizations based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).

Area 3. Contingency Planning (NIST Control Set CP): While the Judicial Council has partially implemented individual functions specified by this set of controls, others must still be implemented or enhanced and formalized under an ongoing disaster recovery program.

- Background: This set of controls specifies the establishment of (i) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (ii) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. Organizations are responsible for the implementation of an information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

Area 4. Security Program Management (NIST Control Set PM): While the Judicial Council has partially implemented individual functions specified by this set of controls, others must still be implemented or enhanced and formalized under an ongoing security program that is properly staffed and whose work assignments do not include the same development, administration and support tasks that they are responsible for monitoring and reviewing.

- Background: This set of controls specifies the need to for a formalized security program within the organization. Such a program includes the establishment of a security program plan, the appointment of an Information Security Officer, and the establishment of information security resources. Additionally, measures of performance are to be established, along with a risk management strategy, insider threat program, testing, training and monitoring capabilities, and the establishment of a threat awareness program.

Area 5. Media Protection (NIST Control Set MP): While the Judicial Council has partially implemented individual functions specified by this set of controls, the establishment of a formalized data classification program is still outstanding.

- Background: This set of controls specifies the need for specific media protection measures, which include access controls, storage and transport requirements, use restrictions, and handling of media that is commensurate with the security category and/or classification of the information residing on the media.

While the Judicial Council has implemented some tools internally to address a recommendation to follow industry-standard best practices, these same capabilities must be implemented within the courts. There is also a need to implement risk assessments. In order for these assessments to be objective, they should be performed by qualified external parties. As a result, these assessments will result in costs that are unable to be covered within the Judicial Council's existing budget. And finally while the Judicial Council has partially implemented individual functions specified by the FISCAM set of controls, others must be implemented, enhanced and formalized under new programs for disaster recovery and data classification. This will ensure that the programs are properly staffed and that the work assignments do not include the same development administration and support tasks that they would be responsible for monitoring and reviewing.

Implementation of Information Systems Control Enhancements BCP Request

This request for funding of $2.4 million in FY 2015-16 and $1.1 million ongoing in subsequent years is to address the California State Auditor recommendations. The funds requested will be used as follows:

Area 1: Audit and Accountability

- Deliverable: Implementation of user access auditing tools within the courts.
- Budget: $615,000 one-time and $47,000 ongoing
- Objective: Using the deployment of user access auditing tools within the Judicial Council as a proof of concept, extend this functionality to the courts via a centrally-funded program that does not divert court funding from other priorities. Courts will then have local tools that can collect server log data into a single location where user account changes can be identified and documented. This will give them visibility into the underlying automated logging that shows the date and time of when actual system events were processed.

Area 2: Risk Assessment

- Deliverable: Establishment of periodic performance of organizational risk assessments within Judicial Council
- Budget: $210,000 one-time and $208,000 ongoing
- Objective: Ongoing risk assessments would 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.

Area 3: Contingency Planning

- Deliverable: Implementation of disaster recovery infrastructure and capabilities within the Judicial Council.
- Budget: $885,000 one-time and $500,000 ongoing
- Objective: The Disaster Recovery program will ensure service continuity by addressing potential disruptions. These may include relatively minor interruptions such as temporary power failures as well as major disasters such as fires, natural disasters and terrorism. All of which might require re-establishing operations at a remote location.

Area 4: Security Program Management

- Deliverable: Implementation of a formalized information security program within the Judicial Council.
- Budget: $365,000 one-time and $345,000 ongoing
- Objective: The security program will improve the Judicial Council's ability to implement and enforce best practices, and to keep pace with evolving threats which can impair technology systems and place the agency at a greater risk for compromise and data loss.

Area 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 will ensure that data is stored, labeled and safeguarded at a level commensurate with its classification.

Staffing:

This request also proposes funding to support 3.0 positions which are included in the above totals as follows:

1. Disaster Recovery program (Area 3 – Contingency Planning)
    - If we receive approval for the Disaster Recovery program, it will result in a workload increase that will require the addition of 1.0 Business System Analyst.
    - **Position 1**: The Business Systems Analyst will be assigned to the Network Infrastructure and Security Architecture Services group, and will be responsible for the ongoing administration of the disaster recovery program. Duties include:
        - Delivery of IT Service Continuity and Disaster Recovery Services
        - Disaster Recovery Planning
        - Disaster Recovery Testing
        - Disaster Recovery Reporting and Reviewing
    - Lack of sufficient staff and financial resources for Disaster Recovery may result in the inability for the organization to maintain continuity of operations, and to reliably recover from catastrophic outages in a timely and effective manner.
2. Security program (Area 4 – Security Program Management)
    - If we receive approval for the implementation of a formalized information Security Program, it will result in a workload increase that will require the addition of 1.0 Supervising Analyst B and 1.0 Business Systems Analyst.
    - **Position 2**: The Supervising Analyst B will be assigned to the Network Infrastructure and Security Architecture Services group, and will be responsible for developing and overseeing the establishment and maintenance of a security operation. Current resources are insufficient to meet the needs of this new responsibility. These duties include:
        - Security program administration
        - Assurance and training of JCC staff
        - Develop, maintain and oversee information security policies, procedures and control techniques
        - Reporting of effectiveness of security program to JCC senior management
        - Hire, train and manage associated staff

- **Position 3**: The Business Systems Analyst will be assigned to the Network Infrastructure and Security Architecture Services group, and will be responsible for seeing that compliance standards are enforced and working with external agencies to communicate threats and vulnerabilities. This will allow the JCC and CCTC to have business continuity in a secure fashion. These duties include:
    - Protection of information and information assets
    - Managing vulnerabilities
    - Managing threats and incidents
    - Reporting issues to senior JCC management and/or external agencies (US-CERT, State CIO)
- Lack of sufficient staff and financial resources for security program administration may result in elevated risk data loss or compromise, and would limit the ability to stay abreast of and adhere to industry best practices.

A&E Committee Meeting
Statewide Data Exchanges
FY 2015-16 BCP

FY 15-16 BCP Program Background and Staffing Status

The Data Integration Team currently has a staffing level of a Senior Business Systems Analyst and utilizes contract resources for a Project Manager and three developers. There is currently a vacancy for a Senior Technical Analyst.

Current Year Conditions and Projects:

Data Integration staff is currently occupied with multiple development, enhancement, maintenance and infrastructure improvement tasks. These include:

- Modifications to the Judicial Branch Statistical Information System (JBSIS) to better reflect actual Trial Court workload so that these statistics provide more accurate input into the Workload Allocation Funding Model
- Development and testing of an interface and additional functionality between the California Courts Protective Order Registry (CCPOR) and the FAmily Court Case Tracking System (FACCTS). This helps automate entry of case data into the courts' Case Management Systems, it enables clerks to record and print court orders, eliminates tedious double data entry, supports the ability to send court orders electronically to the California Law Enforcement Telecommunications System (CLETS) and overall, decreases the time it takes to deliver court orders to all parties.
- Maintaining the data integration framework so that production software will continue to receive vendor support and run on hardware and operating system software that is currently supported by their respective vendors
- Decommission hardware and software infrastructure to reflect the current needs of courts that have changed Case Management Systems, e.g., Merced
- Maintaining existing infrastructure and interfaces selected partners, to support the applications used by 47 of the 58 trial courts, including CCPOR/FACCTS, CCMS v3, JBSIS, and Phoenix.

There is fractional developer bandwidth that can be managed, for example, deferring infrastructure improvements. This will allow the current staff of a single Senior Business Systems Analyst FTE, a contract Project Manager and three contract Developers to maintain the proposed exchanges with the five partners identified below because the maintenance effort (excluding significant enhancements) should be less overall effort than the development effort. There is insufficient bandwidth to complete any single one of these new, proposed exchanges without sacrificing current projects already underway.

Statewide Data Exchange BCP Request:

This request is to fund the development, testing and implementation of five critical statewide data exchanges between the Superior Courts of California and:

- California Department of Social Services – Child Welfare System
- California Department of Motor Vehicles – DMV Query/Update functionality
- California Highway Patrol – Citation Exchange Implementation
- California Department of Justice – Disposition Reporting Exchange Implementation
- Judicial Council – JBSIS Portal Replacement and CMS Reporting

The FY15-16 funding request is to fund $1,620,000 in contract staffing costs, $320,000 in one-time software license costs, and $200,000 in data center operational costs (which includes hardware). In FY16-17, to complete the effort, there is a funding request for $1,660,000 in contract staffing costs, $64,000 in annual software maintenance and $400,000 in data center operational costs. For the subsequent 3 years, there is a $64,000 annual software maintenance cost and a $300,000 projected annual data center operational cost.

Over a five-year horizon, there the costs are as follows

	FY 16-17	FY 17-18	FY 18-19	FY 19-20	FY 20-21
Staffing	$ 1,620,000	$ 1,660,000			
Software	$320,000				
Software Maintenance		$64,000	$64,000	$64,000	$64,000
Data Center	$200,000	$400,000	$400,000	$400,000	$400,000
Yearly Total	$ 2,140,000	$ 2,124,000	$ 464,000	$ 464,000	$ 464,000

Table 1 One-time and recurring costs over 5 years

Total costs over five years is $5,656,000

Staffing Profile

For the five development/implementation projects with these Justice Partners, the mix of Senior Business System Analysts/Project Managers, Developers and Quality Assurance Staff (Testers), will change over time with the progress of the projects, as follows:

			FY 16-17		FY-17-18	
		Est. Hrly Rate	Q1/Q2	Q3/Q4	Q1/Q2	Q3/Q4
CDSS	PM/BSA	100	0.5	0.5	1	1
	DEV	120	0	0.5	2	2
JBSIS	PM/BSA	100	0.5	0.5	0.25	0.25
	DEV	120	0	1	1	1
CADOJ	PM/BSA	100	0.5	0.5	0.25	0.25
	DEV	120	0.25	0.25	0.25	0.25
CHP	PM/BSA	100	0.5	0.5	0.5	0.5
	DEV	120	0.5	0.5	0.5	0.5
DMV	PM/BSA	100	0.5	0.5	0.25	0.25
	DEV	120	2	0.25	0.25	0.25
Shared Testing	Tester	100	1	2	2	1
Staffing Total	PM/BSA		2.5	2.5	2.25	2.25
By Role	DEV		2.75	2.5	4.0	4.0
	Tester		1	2	2	1
Rounding:	PM/BSA		3	3	2	2
	DEV		3	3	4	4
	Tester		1	2	2	1

Table 2 TwoYear Staffing Profile by Position

The Project Manager/Senior Business Systems Analyst position will be responsible for managing the project and ensuring the business requirements are understood and clearly documented. This includes:

- Documenting the project scope and gaining consensus from all the project stakeholders
- Developing and maintaining the project schedule, enumerating the tasks to be done, assigning resource to those tasks and modifying the schedule as required
- Gathering, understanding and documenting the business requirements for the project
- Developing illustrative examples of how the system will be used to

confirm the business requirements
- Communicating with stakeholders throughout the project regarding the project progress, issues and risks
- Participating in the development of the technical solution design to ensure the technical solution will adequately solve the business problem consistent with the agreed upon project scope
- Work with data center staff to document the work order requirements to purchase and deploy hardware and software as documented in the design documents
- Managing the timeline, budget and the status of all deliverables from the developers, the testers and other required stakeholders
- Ensuring operational support is trained and ready for deployment of the solution
- Communicating with users, support staff and business stakeholders about the implementation of the solution
- Conducting post-release assessments to learn lessons for future deployments

The Developer position will be responsible for participating in the requirements process to understand the business problem, developing an efficient and effective design for the data exchange, implementing and performing initial testing of that design, and participating in the deployment of the solution and providing knowledge transfer and technical support post release. This includes:

- Participating in the requirements gathering to understand the business problem and ensure a solution is possible with the available technology
- Developing design documentation which lays out the hardware infrastructure and connections in order to carry out the solution
- Coding and/or configuring a solution to solve the various business scenarios consistent with the business requirements
- Performing initial testing to ensure the solution correctly performs according to the specifications/requirements. Documenting those test results.
- Developing deployment instructions/release notes so that the solution can be deployed successfully
- Performing knowledge transfer and documenting support solutions for existing contract developers so that they can support the data exchange after the conclusion of development

The Tester positions are shared across all five of the data exchange projects. They will be responsible for developing test plans, test cases, and test scripts which will demonstrate each of the requirements. This includes:

- Developing test plans, test cases and test scripts based on each of the business requirements
- Ensuring test data are available to the development team which illustrate

the type and volume of the data to be encountered when the solution is in production
- Validating the basic test results after the initial development and perform more advanced testing to ensure the solution is sufficiently robust.
- Working with the business subject matter experts to ensure the user acceptance testing is sufficient
- Performing system or integration tests to ensure all the components work together
- Performing tests of the whole system as changes are made during the development process to ensure fixes in one area do not cause issues in another area

Courts need to exchange data with their Justice Partners in order to carry out their mission: DMV records need querying and updating to determine appropriate fines; case dispositions need reporting to the DOJ to ensure records are accurate, from the original arrest records through to the case disposition. Summary statistics need to be transmitted to the Judicial Council so that funds to the courts can be allocated using a data-driven workload model; citation information from the CHP can be entered into court systems much faster and more accurately using an electronic data exchange; courts and the DCSS need to exchange information to better serve their constituencies.

The need for statewide data exchanges is urgent because new case management systems (CMS) to which courts are migrating do not yet have data exchanges integrated into the CMS. The project staffing profile reflects the urgency for these interfaces and assumes the development work for these statewide interfaces will be done in parallel. Staffing costs can be reduced and hardware purchases could be extended over a longer period of time if it's deemed that the interfaces are done in a more serial fashion. However, this delay in implementation may cause some courts to seek individual court solutions, increasing overall costs to the branch and to the state. If neither a statewide data exchanges nor multiple electronic exchanges can be funded, courts may require additional staffing to process the large volume of data that would have been handled through these electronic data exchanges.