

**Office of Information Security and
Privacy Protection**

Information Technology Capital Plan



**Information Technology Capital Plan,
Plan Year 2009-10 through 2013-14
Executive Approval Transmittal**

Department Name

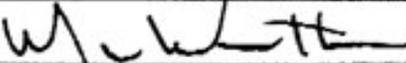
Office of Information Security and Privacy Protection, part of the State and Consumer Services Agency

APPROVAL SIGNATURES

I am submitting the attached Information Technology Capital Plan as required by the State Administrative Manual Section 4904.

I certify that the IT Capital Plan was prepared in accordance with State Information Management Manual section 57 and that the proposed IT projects are consistent with our business strategies and information technology strategy.

I have reviewed and agree with the information in the attached Information Technology Capital Plan.

Chief Information Officer		Date Signed
		
Printed name:	Andrew Armani	
Information Security Officer		Date Signed
* UNAVAILABLE @ time of submittal		
Printed name:	Manolo Platin	
Budget Officer		Date Signed
* UNAVAILABLE @ time of submittal		
Printed name:	Rene Gutierrez	
Department Director		Date Signed
		
Printed name:	Mark Weatherford	7/30/08

DEPARTMENT IT CAPITAL PLAN

Department Name and Org Code:

Office of Information Security and Privacy
Protection (OISPP) - 0510

Plan Year:

2009-10 through 2013-14

1. Summarize your organization's business goals and objectives below:

The California Office of Information Security and Privacy Protection (OISPP) is located within the State and Consumer Services Agency (SCSA). The mission of OISPP is to unite consumer privacy protection with the oversight of government's responsible management of information to ensure the trust of Californians.

The OISPP provides services to consumers, recommends practices to business, and gives policy direction to state government through the Office of Privacy Protection and the Office of Information Security.

2. What are your organization's plans to upgrade or replace your IT infrastructure for the following? When responding, please indicate the timeframes of your intended upgrade or replacement efforts.**2.1. Hardware**

New Personal Computers (PC) as of mid 2008. For scheduling and budget purposes, the OISPP anticipates the need for refreshing the PCs in early 2011 (fiscal year 2010-11). Actual replacement will be based on problems and/or deficiencies with the equipment instead of the passage of a fixed number of years.

The Department of Technology Services (DTS) provides the OISPP's servers and we follow their maintenance and refresh schedule.

2.2. Software

New software licenses as of mid 2008. For scheduling and budget purposes, the OISPP anticipates the need for software upgrades in early 2010 (fiscal year 2009-10). Actual upgrades and/or replacement will be based on problems and/or deficiencies with the software instead of the passage of a fixed number of years.

The DTS provides the OISPP's servers and we follow their maintenance and refresh schedule.

2.3. Network

The DTS provides the OISPP's network telecommunications hardware and we follow their maintenance and refresh schedule.

3. Existing Approved Reportable IT Projects

Provide the following information regarding your existing approved reportable IT projects on Table 1 on the following page:

- **Existing IT Project;**
- **Approved Project Cost;**
- **Project Number; and**
- **Implementation Date**

4. Proposed IT Projects

After each proposed IT project has been documented by answering questions 4.1 through 4.15 of the attached IT Project Proposal Form, provide the following information on Table 2 on the following page:

- **The name of each proposed IT project;**
- **The priority ranking;**
- **The FSR submission date; and**
- **The estimated cost**

Table 1-Existing Approved Reportable IT Projects Summary by Department

Existing IT Project	Approved Project Cost*	Project Number	Implementation Date
Enterprise-wide Online Cyber Security and Privacy Awareness Training System (Non reportable project included for transparency and disclosure.)	\$235,863	Internal FSR approved 08/04/2008	02/01/2010
Threat and Vulnerabilities Management Program (Non reportable project included for transparency and disclosure.)	Not applicable	OISPP is in the process of hiring a consultant to establish an enterprise program to test web applications and other agency systems for known security vulnerabilities	Unknown
IT Project Security Oversight (Non reportable planning effort included for transparency and disclosure.)	\$580,000 (FY 08-09 = \$290,000 / FY 09-10 = \$290,000)	Not applicable	Early 2009

***Note:** If a Special Project Report (SPR) was submitted for review in July 2008 that includes project costs that differ from the last approved project document, enter both the last approved project cost and the revised project cost from the SPR under review.

Table 2-Proposed IT Project Summary

Proposed IT Project	Priority Ranking	FSR Submission Date	Estimated Total Cost
Enterprise-wide California Information Sharing and Analysis Center (CA-ISAC) (Non reportable planning effort included for transparency and disclosure.)	1	OISPP plans to develop an information sharing portal for all state government organizations; estimated submission 07/2009	Unknown
Enterprise-wide Online Incident Reporting System (Non reportable planning effort in 2008-09 included for transparency and disclosure.)	2	OISPP is in the process of hiring a consultant to write the FSR; estimated submission 07/2009	Unknown

PROPOSED IT PROJECTS

Complete this IT Project Proposal Form (questions 4.1 through 4.15 below) for each proposed IT project that meets the definition of a reportable project as defined in the State Administrative Manual Section 4819.37:

4.1 Proposal name and priority ranking:

Enterprise-wide California Information Sharing and Analysis Center (CA-ISAC) - Priority Ranking 1

4.2 Description of the proposed IT project:

Develop and implement a secure CA-ISAC, a secure Web site that is available to authorized state and local government employees, and provides intelligence information sharing capabilities and up-to-date vulnerability and threat notifications. This is not considered a project since Multi-State ISAC (MS-ISAC) provides this as a service. It would require the consultant to collect requirements and work with MS-ISAC to develop it to meet California's needs. This is a non reportable planning effort in 2008-09 included for transparency and disclosure.

4.3 Which of your department's business goals and objectives does this project support, and how?

This project will support the OISPP's purpose to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect consumer privacy to ensure the trust of the residents of this state. The project further supports the OISPP's mission to promote and enhance the state agencies' risk management and privacy programs through education and awareness.

See response to Question 4.4 for how CA-ISAC supports these goals and objectives.

4.4 What are the expected business outcomes or benefits of the proposal as they relate to your organization's business goals and objectives?

The project will enhance the State's ability to prevent, detect, prepare for, and respond to cyber security incidents by providing a low cost tool for agencies to obtain information and share problems and solutions with other authorized state and local government employees. It also compliments the United States National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.

4.5 The following are from the State's IT strategic plan. Check the appropriate box(es) to identify the goals this proposal supports:

- Supporting and enhancing services for Californians and businesses**
- Enhancing information and IT security**
- Reducing state operational costs (leveraging, consolidation, new technology, etc.)**
- Improving the reliability and performance of IT infrastructure**
- Enhancing human capital management**
- Supporting state and agency priorities and business direction**

PROPOSED IT PROJECTS CONTINUED - CA-ISAC

- 4.6 Is the proposal consistent with your organization's Enterprise Architecture?**
 Yes
 No

If no, please explain why the deviation from the organization's Enterprise Architecture is necessary.

- 4.7 Will the proposed system collect, store, transmit, or exchange confidential or sensitive information?**
 Yes
 No

- 4.8 If this proposal is conceptually approved, what is the estimated date (mm/yyyy) the FSR will be submitted?**

If required, the FSR submittal date is estimated to be 07/2009.

- 4.9 What is the estimated project start date (mm/yyyy) if the FSR is approved?**

The project start date is to be determined.

- 4.10 What is the duration of the proposed project?**

The project duration is to be determined.

- 4.11 Will the proposed project utilize the existing infrastructure?**
 Yes
 No

If no, please explain.

- 4.12 Is the proposal related to another proposal or to an existing project?**
 Yes
 No

If yes, describe the related proposal or project and how it is related:

- 4.13 Describe the consequences of not doing this proposed project at the planned timeframe:**

California will continue to lack a coordinated vehicle for disseminating and sharing cyber threat information with state and local government and higher education organizations. This will result in continued inconsistencies in responding to cyber threats throughout the state.

PROPOSED IT PROJECTS CONTINUED - CA-ISAC

4.14 Check the appropriate box(es) to identify the proposal's funding strategy:

- Augmentation needed
- Redirection of existing funds
- Other (describe): To be determined

4.15 What are the estimated cost and funding source(s) by fiscal year through implementation (information should be provided in the following format):

Fund Source	2008/09	2009-10	2010-11	2011-12	2012-13	2013-14 and future	Total
General Fund							
Federal Fund							
Special Fund*							
Total	\$100,000	\$10,000	\$10,000	\$10,000	\$10,000	\$10,000	\$150,000

The above amount is estimated for initiating the business program.

*** Note: Identify the fund source and if the department is the sole user of the fund.**

PROPOSED IT PROJECTS

Complete this IT Project Proposal Form (questions 4.1 through 4.15 below) for each proposed IT project that meets the definition of a reportable project as defined in the State Administrative Manual Section 4819.37:

4.1 Proposal name and priority ranking:

Enterprise-wide Online Incident Reporting System - Priority Ranking 2

4.2 Description of the proposed IT project:

Evaluate the feasibility of a statewide online incident reporting system by hiring a consultant to lead a feasibility study effort and document the fully defined business objectives, alternatives, solutions, anticipated costs, schedule, etc. This is a non reportable planning effort in 2008-09 included for transparency and disclosure.

4.3 Which of your department's business goals and objectives does this project support, and how?

This project will support the OISPP's purpose to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect consumer privacy to ensure the trust of the residents of this state.

The project further supports the OISPP's mission to create, issue, and maintain policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.

See response to Question 4.4 for how the Online Incident Reporting System supports these goals and objectives.

4.4 What are the expected business outcomes or benefits of the proposal as they relate to your organization's business goals and objectives?

The project will enhance the State's ability to prevent, detect, prepare for, and respond to cyber security incidents by enhancing interoperable communications by clearly defining the collective needs for information collection, sharing and reporting as it relates to cyber security incident management and determining a appropriate course of action for the establishment of more effective methods and/or solutions.

Establishment of an effective incident management system is consistent with the United State National Strategy for Homeland Security and the California State Strategy Goal 2, Objectives 2.1 and 2.2 by strengthening interoperable communications capabilities and enhancing interoperable communications and the State Terrorism Threat Assessment Strategy and Information Sharing Process.

PROPOSED IT PROJECTS CONTINUED - Enterprise-wide Online Incident Reporting System

4.5 The following are from the State's IT strategic plan. Check the appropriate box(es) to identify the goals this proposal supports:

- Supporting and enhancing services for Californians and businesses
- Enhancing information and IT security
- Reducing state operational costs (leveraging, consolidation, new technology, etc.)
- Improving the reliability and performance of IT infrastructure
- Enhancing human capital management
- Supporting state and agency priorities and business direction

4.6 Is the proposal consistent with your organization's Enterprise Architecture?

- Yes
- No

If no, please explain why the deviation from the organization's Enterprise Architecture is necessary.

4.7 Will the proposed system collect, store, transmit, or exchange confidential or sensitive information?

- Yes
- No

4.8 If this proposal is conceptually approved, what is the estimated date (mm/yyyy) the FSR will be submitted?

The estimated date is 07/2009.

4.9 What is the estimated project start date (mm/yyyy) if the FSR is approved?

The start date is to be determined.

4.10 What is the duration of the proposed project?

Approximately one year.

4.11 Will the proposed project utilize the existing infrastructure?

- Yes
- No

If no, please explain.

PROPOSED IT PROJECTS CONTINUED - Enterprise-wide Online Incident Reporting System

4.12 Is the proposal related to another proposal or to an existing project?

- Yes
 No

If yes, describe the related proposal or project and how it is related:

4.13 Describe the consequences of not doing this proposed project at the planned timeframe:

The OISPP will forfeit Department of Homeland Security (DHS) grant funding for this project if it is not implemented by March 2010. The current manual process will continue.

4.14 Check the appropriate box(es) to identify the proposal's funding strategy:

- Augmentation needed
 Redirection of existing funds
 Other (describe): DHS grant funding

4.15 What are the estimated cost and funding source(s) by fiscal year through implementation (information should be provided in the following format):

Fund Source	2008/09	2009-10	2010-11	2011-12	2012-13	2013-14 and future	Total
General Fund							
Federal Fund							
Special Fund*							
Grant Funds	104,230						
Total	104,230						104,230

The above amount is only the grant funds. At this time, we have not identified what, if any, additional project costs are needed, such as the cost associated with the staff time allocated to this project. The feasibility study will include identifying the required schedule and costs.

*** Note: Identify the fund source and if the department is the sole user of the fund.**

Enterprise Architecture

A.1. Does your organization have documented Enterprise Architecture principles, strategies, or standards to guide decisions on technology projects?

- Yes
- No

As an SCSA sub-agency, the OISPP follows the SCSA’s direction.

A.2. Indicate on Table A-1 below, the completion status of the component Reference Models of your formal Enterprise Architecture efforts. If available, please submit a copy of your Enterprise Architecture document.

Table A-1, Enterprise Architecture Completion Status

Component Reference Model	Status			
	Implemented	Implementation in Progress	Planned or Planning in Progress	Not Implemented and Not Planned
Business				√
Service				√
Technical				√
Data				√

A.3. Describe the governance structure your organization uses to review and approve the Enterprise Architecture and any subsequent changes.

None

A.4. Does your organization have an Enterprise Architect? (if yes, provide their name, telephone number, and e-mail address below)

- Yes
- No

As an SCSA sub-agency, the OISPP follows the SCSA’s direction.

Name:
Classification:
Telephone Number:
E-Mail:

Information Security

B.1. How is your Information Security Officer involved in proposed project development efforts?

The SCSA Information Security Officer reviews, provides input to, and approves proposed IT projects.

B.2. What are your department's core business principles, policies and standards related to information integrity, confidentiality, and availability and the protection of information assets?

Per Chapter 183 of the Statutes of 2007 (Senate Bill 90), the OISPP was created on January 1, 2008, within the SCSA. The OISPP acts as the primary state government authority in ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information. Our Mission is to ensure the trust of Californians by providing statewide strategic direction and leadership in the protection of the State's information assets.

The OISPP practices these principles daily and communicates a similar message to state agencies. For example, our Government Online for Responsible Information Management (GoRIM) emphasizes the need to protect the confidentiality, integrity, and availability of the state's information assets.

B.3. If data within your department is shared with external entities, does your department implement data exchange agreements with these entities?

- Yes
 No

If no, please explain.

OISPP's data is confidential in nature. The bulk of our data is received from other state agencies, such as operational recovery plans and security incident and privacy breach information. The information is kept in locked files and not disclosed. The OISPP provides some statistical information that is not identifiable back to the source in summary reports. Most of these reports are not widely distributed.

Not applicable

B.4. How does your department ensure that software developers and programmers follow standards and best practices for Web, application, and system development?

Neither the SCSA nor the OISPP have software developers or programmers on staff. For contracts, such as internal non-reportable projects, the OISPP crafts requirements to impose state best practices and our Office's confidentiality standards on contractors.

B.5. Does your organization have an Information Security Officer? (if yes, provide their name, telephone number, and e-mail address below)

- Yes
 No

Name: Manolo Platin (SCSA ISO)
Classification: Special Assistant
Telephone Number: (916) 653-3873
E-Mail: manolo.platin@scsa.ca.gov

Workforce Development, Workforce Planning and Succession Planning

C.1. Does your organization have a workforce development plan for IT staff?

- Yes**
- No** In development.

If yes, briefly describe it.

C.2. Check the appropriate box(es) to identify which workforce development tools, if any, your organization is using for IT classifications:

- Training**
- Upward Mobility**
- Mentoring**
- Career Assessments**
- Knowledge transfer program**
- Performance Evaluations**
- Other (please list)**

C.3. Does your organization have a workforce plan for IT staff (i.e., for Rank and File)?

- Yes**
- No** In development.

If yes, briefly describe it.

C.4. Does your organization have a succession plan for IT staff (i.e., for Management)?

- Yes**
- No** In development.

If yes, briefly describe it.

C.5. IT Staffing

Provide the following information in table C-1 on the following page:

- **The name of each IT classification currently in the organization.**
- **The number of staff in each IT classification in the organization.**
- **The number of staff in each IT classification eligible to retire in the next five years.**
- **The percentage of each IT classification eligible to retire in the next five years.**

Table C-1 — IT Staffing

IT Rank and File Staff Classification	Number of IT Rank and File Staff in Classification	Number of IT Rank and File Staff in Classification Eligible to Retire in Next 5 Years	IT Management Staff Classification	Number of IT Management Staff in Classification	Number of IT Management Staff in Classification Eligible to Retire in Next 5 Years
None	0	0	DPM IV	1	1
			DPM II	3	2

Project Management, Portfolio Management and IT Governance**D.1. Does your organization have a process for improving the alignment of business and technology?**

- Yes
 No

If yes, briefly describe it.

Consistent with our mission, the OISPP provides policy direction to state agencies. In this sense, examples of our improving the state's alignment of business and technology include our direction to state agencies for operational recovery plans and for incident management.

D.2. What is the status of implementing a formal portfolio management methodology for technology projects within your organization?

- Implemented (Please describe)
 Implementation in progress (Please describe)
 Planned or planning in progress
 Not implemented and not planned

OISPP does not currently have any reportable technology projects.

D.3. List any automated tools being used for portfolio management. Enter "None" if no automated tools are being used.

None

D.4. What is the status of implementing a standard project management methodology for technology projects in your organization?

- Implemented (Please describe)
 Implementation in progress (Please describe)
 Planned or planning in progress
 Not implemented and not planned

OISPP follows the SCSA's direction.

Project Management, Portfolio Management and IT Governance

D.5. Does the organization require its project managers to be certified, either through a professional organization (e.g., PMI, ITIL) and/or through completion of specified project management coursework:

- Yes
- PMI
 - ITIL
 - Agency-specified project management coursework (identify below)
- No

D.6. Select from the list other areas of training your organization requires of its project managers:

- Fundamental Project Management
 - Systems Development Life Cycle
 - Scheduling tool (identify below)
 -
 -
 - Project Performance Management (e.g., Earned Value Management)
 - Business Process Analysis
 - Requirements Traceability
 - Procurement/Contracts Management
 - Other (identify below)
 -
 -
- None

Although we have no written requirements for project manager training, various members of the OISPP's staff have led successful projects, worked in a project management office, taken systems development life cycle training, performed requirements traceability, and participated in state procurements.

D.7. Describe project-level governance practices, including change management, issue resolution, and problem escalation.

OISPP follows the SCSA's direction.

D.8. Does the project management methodology include processes for documenting lessons-learned and applying these to future projects?

- Yes (Please describe)

OISPP follows the SCSA's direction.

- No