

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



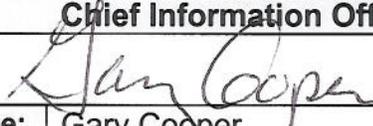
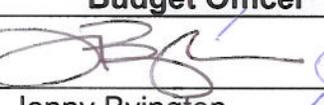
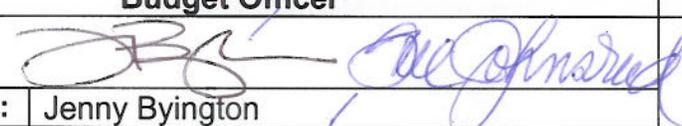
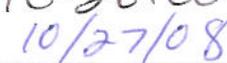
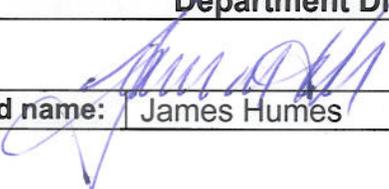
Department Name

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:	Gary Cooper	
Information Security Officer		Date Signed
		
Printed name:	Andy Kraus	
Budget Officer		Date Signed
		
Printed name:	Jenny Byington	
Department Director		Date Signed
		
Printed name:	James Humes	

DEPARTMENT IT CAPITAL PLAN

Department Name and Org Code:

Department of Justice 0820

Plan Year:

2009-10 through 2013-14

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

The mission of the Department of Justice is to provide leadership, information and education in partnership with state and local governments and the people of California to:

- Enforce and apply all of our laws fairly and impartially.
- Ensure justice, safety, and liberty for everyone.
- Encourage economic prosperity, equal opportunity and tolerance.
- Safeguard California's human, natural, and financial resources for this and future generations.

The DOJ carries out its mission through four distinct lines of business, each with its own business goals and objectives:

- Legal services,
- Law enforcement activities,
- Information management, and
- Administrative services.

➤ LEGAL SERVICES

Goal #1: Improve access to critical information and communication for DOJ professional staff, including attorneys, auditors and investigators, from any location at any time.

Objective: Develop a method for attorneys, auditors and investigators to have remote access to case documents, applications/databases, and other on-line resources to perform legal and investigative research from any location at any time.

Objective: Expand DOJ's capability to interact electronically with courts, law firms and other governmental agencies.

Objective: Provide electronic tools that will enable DOJ attorneys to be competitive in the courtroom.

Goal #2: Improve DOJ attorney, auditor, investigator, paralegal and support staff's capability to manage the volumes of paper and electronic data, including voice and video.

Objective: Develop tools and processes to search and preserve data from clients that is received in diverse formats.

Objective: Develop tools, processes, policies, expertise and capacity to preserve, search and present DOJ electronic documents, including emerging formats, such as voice and video data (from cell phones, e-mail, voice mail and other electronic devices).

Objective: Expand capability for electronic storage and increase capability to search litigation documents and information.

Goal #3: Ensure DOJ data assets are secure, without impacting the work of attorneys, auditors, investigators, paralegals and support staff.

Objective: Develop methods to access electronic litigation information from any where at any time with appropriate levels of security.

Goal #4: Leverage existing information resources in legal casework.

Objective: Develop agreements with entities to enable access to systems and information that will enable attorneys, auditors, investigators and paralegals to more efficiently and effectively handle Medi-Cal fraud and other legal cases.

➤ **LAW ENFORCEMENT ACTIVITIES**

Goal #1: Provide cutting-edge delivery of services in forensic science, narcotic investigations, criminal investigations, intelligence, and training to our clients and customers.

Objective: Evaluate processes, methods, and technologies that can improve service delivery quality.

Goal #2: Ensure accurate and timely firearms licensing.

Objective: Develop the processes and technology to enable the efficient and secure transfer and storage of information from citizens, firearms businesses and other public agencies.

Goal #3: Provide timely, accurate and consistent levels of forensic analysis services to all service regions.

Objective: Monitor the volumes of regional laboratory casework and adjust workload in response to the distribution of California population and crime areas.

Objective: Evaluate opportunities to use technology to perform work more efficiently and effectively to offset staffing and infrastructure deficiencies.

Goal #4: Ensure the integrity of gambling in California by investigating organized crime, embezzlement, fraud, loan sharking, illicit narcotic trafficking and other gaming-related crime.

Objective: Utilize technology to make operations more efficient and to provide more timely service to clients.

Goal #5: Provide leadership, coordination, and support to law enforcement agencies in combating drugs, illegal weapons, and violent crime in California.

Objective: Develop and implement innovative information technology systems, surveillance and analytical tools, and business processes to support operational needs and enhance service delivery.

Objective: Develop and improve information technology systems to monitor controlled prescription drugs, chemicals and other substances.

Goal #6: Provide expert level criminal investigation services to law enforcement clients and the public.

Objective: Provide agents with access to technology and information systems that will enable them to maximize their time while performing investigative work in the field.

Objective: Utilize technologies and systems to help meet an increasing demand for service without increasing existing personnel.

Goal #7: Collect and disseminate timely information regarding organized crime, gang, and terrorist activities to local, state and federal criminal investigators and prosecutors.

Objective: Evaluate processes, methods and technologies that can speed and simplify the secure exchange of relevant information.

Objective: Facilitate collaboration with local, state, and federal law enforcement agencies to ensure officer safety and maximize the ability to detect, prevent, investigate, apprehend, prosecute, and respond to traditional criminal and terrorist activity.

Objective: Acquire new technologies to provide the best products to investigative analysts, such as data warehouse and analysis tools, entity recognition software, and mapping applications.

➤ **INFORMATION MANAGEMENT**

Goal #1: Shift the emphasis of information management from control to value creation/delivery.

Provide practices, tools and the environment that promotes the delivery of value and enables excellence in customer/partner service.

Objective: Design and implement Customer Relationship Management frameworks that promote a better understanding of DOJ's customers/partners and enable high quality responsive service in alignment with the directions and priorities established by DOJ.

Objective: Design and implement a Project Office that focuses on value driven portfolio management, streamlining and standardizing project management approaches/tools, and raising the competency level of project managers within DOJ.

Objective: Design and implement a new work request mechanism that updates and simplifies work requests for customers/partners while at the same time enabling expanded visibility, accountability and quality of the responses to the requests.

Goal #2: Modernize and simplify DOJ's underlying technology infrastructure.

Develop and implement strategies to enable the ongoing optimization of the value generated by DOJ's technology investments.

Objective: Reduce the maintenance cost of maintaining duplicate mission critical environments by expeditiously completing the migration off the Unisys mainframe.

Objective: Leverage state and federal enterprise architecture approaches and frameworks to enhance the quality of DOJ's future technology investments and work efforts.

Objective: Update and upgrade the DOJ's disaster recovery and business continuation capabilities to preserve and enhance the availability of services and information it provides to the state's citizens and criminal justice community.

Goal #3: Enhance integration with criminal justice partners.

Improve criminal justice effectiveness by enhancing and expanding the integration of DOJ systems and information with other criminal justice systems and information.

Objective: Expand and enhance systems-to-system integration within the criminal justice community.

Objective: Explore the feasibility and viability of building (and possibly hosting) a law enforcement records management application that seamlessly integrates with DOJ's applications and fills gaps in small and medium-size agency information management capabilities.

Objective: Leverage state identity management approaches and frameworks to simplify and expand access to criminal justice information resources.

Objective: Leverage state service oriented architecture approaches and frameworks to streamline and expand access to criminal justice information resources.

Goal #4: Enrich information service offerings.

Promote and enable expanded information sharing in the criminal justice community.

Objective: Expand information exchanges (including non-DOJ exchanges) within the criminal justice community.

Objective: Promote and enable simplified capture and exchange of cite and release arrest information between law enforcement, DOJ and the courts

Objective: Expand/facilitate/simplify access to investigative/intelligence tools and information.

Objective: Facilitate anytime anywhere access (within security constraints) to DOJ information resources.

Objective: Improve quality, timeliness and usability of statistical information.

➤ **ADMINISTRATIVE SERVICES**

Goal #1: A high performance staff - Develop and implement procedures and practices that encourage highly developed core competencies and technical knowledge, high morale, and fully-trained and effective employees at all levels.

Objective: Assess, train, and develop staff members to be proactive, innovative, customer oriented and highly knowledgeable in all aspects of their job.

Objective: Provide the practices, tools and environment that promote excellence in work products and helps attract quality employees.

Objective: Encourage the development of a diverse and culturally aware workforce that addresses the ever-changing California demographics.

Goal #2: Effective Organizational Systems and Processes - Develop and maintain systems, processes, and procedures that maximize the use of our resources and knowledge and help us provide excellent products and services for the DOJ.

Objective: Evaluate and implement the appropriate management information systems.

Objective: Evaluate, improve and streamline DAS internal processes and procedures.

Objective: Improve intra-divisional collaboration and communication.

Objective: Evaluate division resources and effectively match with unit organizational and developmental needs.

Objective: Develop an effective system to ensure both the sharing and retention of critical institutional knowledge.

Goal #3: Proactive Customer Service - Collaborate and develop partnerships with our customers and stakeholders at all levels to provide the information and support they need to accomplish our mutual goals.

Objective: Establish proactive DAS policies that balance customer requests and DOJ resources.

Objective: Establish methods for DAS to better understand program needs and functions.

Objective: Establish a method for recognizing and rewarding employees who deliver excellent customer service.

Objective: Develop and implement methods for encouraging decision-making and problem solving at the lowest appropriate level.

Objective: Improve communication between internal and external customers at all levels and in all units.

Goal #4: Ongoing quality improvement - Anticipate and respond to new opportunities and challenges by regularly reviewing our strategic and operational plans and continually asking the question, "How can we make this better, faster, easier?"

Objective: Create an effective process to integrate, assess and update strategic and unit operational plans.

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

- Storage Refresh – 2012 (SAN and Virtual Tape)
- Disaster Recovery Refresh and Expansion - 2012
- Cal-ID Refresh – 2011
- Mainframe migration to open systems – 2013
- Server Refresh - Unix/Linux/Windows servers – staggered, replace after 5 years (includes CLETS and CJIS systems)
- Desktops – staggered, replace after 5 years
- Facilities (UPS, and other power/AC devices) - staggered

2.2. Software

- Mainframe legacy application migration to open systems/relational db – 2013
- E-Business suite refresh – 2013
- Oracle upgrade - continuous
- Unix upgrade or migration to Linux - tbd
- MS Office upgrade - continuous
- ProLaw email integration - tbd
- Utilities (security, other monitoring tools) - staggered

2.3. Network

- Network Refresh - 2012

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 4.16 through 4.30 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
Automated Criminal History Redesign	\$34,829,000 SPR 3: \$39,958,136	0820-132	June 2008 SPR 3: December 2009
Network Encryption	\$8,493,000	0820-161	October 2008
VCIN Renovation	\$10,261,697 SPR 3: 10,282,000	0820-162	March 2010 SPR 3: April 2009
CJIS Redesign	\$22,350,318	0820-171	December 2010
CLETS Migration	\$9,356,000	0820-172	August 2008
Disaster Recovery	\$303,000	820-180	June 2007
CJIS Technology Refresh 2006	\$15,592,288	0820-189	November 2008
Megan's Law Internet Legislative Enhancements	\$89,771	0820-191	June 2010
DNA Live Scan	\$2,421,000	0820-192	December 2008

***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
EPAS/EMMA Replacement	2	Fall 2008	~\$2,000,000
Document Management (includes ProLaw/email integration, record retention, e-discovery)	1	Winter 2008 - 2009	~\$3,000,000

PROPOSED IT PROJECTS

For the last few years the DOJ has been focused on a several major projects that are scheduled to complete in the next two years. This project set includes:

- Automated Criminal History Redesign
- CJIS Redesign
- CLETS Migration
- VCIN Renovation
- Network Encryption
- DNA Live Scan
- CJIS Technology Refresh

These projects have and will require a great deal of attention and focus to complete. For this reason we do not anticipate adding significant new projects until later in the five-year period unless we have legislative/legal requirements and/or compelling needs. At this point in time our vision of future projects is not mature enough to provide detailed project proposals for each one. Thus we have opted to provide a hybrid response to the OCIO Proposed IT Projects section. The first part includes a list of potential projects. These are significant projects that may become proposed projects in the future. The second part includes the few new major projects that we are now pursuing. These projects each have a completed Proposed IT Project Proposal. This is a relatively small set by design.

Part I: Potential Projects – Too early to include as a Proposed Project

- Financial Information System for California (FI\$CAL) – if this statewide project to implement an integrated financial management system is approved DOJ will be part of the initial agencies for deployment --- dependent upon State Initiative
- MyCalPAYS (21st Century Project) – this statewide project will implement a new Human Resources Management/Payroll system that may require interface development with DOJ systems
- Compliance with Title 1 of the Adam Walsh Child Protection and Safety Act of 2006, the Sex Offender Registration and Notification Act – this is a large undertaking which could potentially cost in excess of \$30,000,000 – before it becomes a proposed project more clarity on requirements is needed --- dependent upon Federal Clarifications
- Expanded Disaster Recovery Capabilities – possible site change – this will expand protection for Livescan (fingerprint submission and searching), email, legal case management, investigative/intelligence applications/data, and communications applications
- CJIS Redesign Phase II – migration of the remaining Criminal Justice Information Systems off the Unisys Mainframe – APS, MUPS, NFE --- submission of proposal content is dependent upon lessons learned in CJIS Redesign Phase I – FEAF, SRF, DVROS, SVS, WPS, AFS
- Criminal Justice Identity Management Framework – will establish an identity management framework to be used by DOJ and law enforcement – criminal justice community at-large -- more research needed before proposal is made

- Accelerated Reporting of Offender Data (AROD) – simplify and improve the collection and use of Unified Crime Reporting information – leverage NIEM – pursue integration with local law enforcement systems – grant application has been submitted
- Intelligence Systems Coordination – Mission Suite – completion of an intelligence “workbench” that integrates intelligence tools into a seamless integrated work environment ---- grant application has been submitted
- Modernize the Information Expedite Program (IEP) – modernize the 7x24 IEP Command Center and Teletype Center at DOJ – current processes are paper intensive and core technologies go back 30+ years – the Command Center supports law enforcement around the state --- development of strategies for improvement are in the very early stages

Part II: Proposed IT Projects

PROPOSED IT PROJECT #1: Document Management

4.1. Proposal name and priority ranking:

Document/Data Management

Rank = 1

4.2. Description of the proposed IT project:

This project may be broken into three or more projects. The overall purpose of this project is a complete review and upgrade of DOJ’s existing technology and processes used for managing data. This includes e-mail, documents, memos, etc. The project will review migrating the department’s current e-mail system to Microsoft Exchange - Outlook in order to integrate with the department’s legal case management application, ProLaw.

ProLaw is an off-the-shelf product for managing legal cases, attorney time, billing, etc. It provides integration with Microsoft Exchange that will enable the department’s attorneys to be more productive.

At the same time, a new data archive solution that includes e-mail will be considered. This will enable us to be better prepared for disaster recovery, support e-discovery needs and to better meet state and federal guidelines in data retention.

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

This project supports the department’s goals to provide improved technical capabilities for DOJ staff, to align with the OCIO goals, and provide product/application integrations for DOJ staff to reduce costs.

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 ability of the DOJ attorney and legal staff to take advantage of Microsoft Exchange integration with their ProLaw application to eliminate or minimize a significant amount of the manual tasks. This in turn will make the attorneys and legal staff more productive.

To provide reliable capabilities and effective e-discovery capabilities, to provide integration of Microsoft Exchange with existing Microsoft software being used by all DOJ staff and ensure effectiveness and usefulness of the department's data storage and retention.

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?

Winter of 2008 - 2009

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

Summer/Fall of 2009

4.10. What is the duration of the proposed project?

1 to 2 years

4.11. Will the proposed project utilize the existing infrastructure?

- Yes
- No

If no, please explain. Yes and no, because the department's existing network backbone (WAN and LAN) already in place will be used.

We will consider consolidating the number of e-mail and file storage servers statewide and installing new servers and additional storage as needed.

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:

Impacts the legal staff's ability to complete required work in an effective and timely manner.

Increased costs due to the need to upgrade existing systems that most likely would be replaced with this project.

Inability to effectively and quickly respond to court required e-discovery and litigation hold requirements.

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

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

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	2009-10	2010-11	2011-12	2012-13	2013-14 and future	Total
General Fund		2,000,000	1,000,000			
Federal Fund						
Special Fund*						
Total						

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

PROPOSED IT PROJECT #2: Evidential Portable Alcohol System (EPAS) Replacement Project

4.16. Proposal name and priority ranking:

Evidential Portable Alcohol System (EPAS) Replacement Project

Priority = 2

4.17. Description of the proposed IT project:

The Bureau of Forensic Services (BFS) owns over 1,100 EPAS units making it the largest Portable Evidential Breath Testing (PEBT) program in California and the first of its kind in the nation. The current EPAS units were developed and placed in the field in 2002, and are at the end of their useful life expectancy of 5-7 years. The Office of Traffic Safety has awarded BFS a grant to purchase new devices, and to enhance the existing IT infrastructure to support the new devices, namely the EPAS Maintenance and Management Application (EMMA), EPAS Oracle Service Manager (EOSM), Bureau Wide Forensic Management System (BWFMS), and BFSInfo Web application.

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

This project supports the BFS business goal to provide timely, accurate blood and breathe alcohol analysis, billing and reporting to all BFS service regions.

Specific objectives of this project are:

- Upgrade the existing EPAS PEBT Data System (PDS) and supporting IT infrastructure to support the new PEBT device
- Meet all necessary department network security and data integrity standards
- Meet state and federal laws for privacy and data security
- Meet the needs of law enforcement to improve breath analysis time and increase the 'ease of use' of the PEBT devices by officers in the field
- Integrate PDS with existing forensic data information systems, BWFMS and BFSInfo Web

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

- Begin the pilot program utilizing the new PEBT devices by October 1, 2010
- Provide greater accuracy of forensic alcohol testing locations for BFS billing services to recover analysis costs from local law enforcement agencies
- Increase the speed and security of reporting and publishing analytical results to the California Highway Patrol, local law enforcement agencies, Department of Motor Vehicles and District Attorneys
- Increase security of confidential data and promote centralization of forensic analysis information

- Support BFS program and law enforcement partners in raising public awareness of the use of PEBT devices and PDS system through technical assistance with training and information exhibits

4.20. 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

4.21. 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.

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

- Yes
- No

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

October 2008

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

January 2009

4.25. What is the duration of the proposed project?

3 years

4.26. Will the proposed project utilize the existing infrastructure?

- Yes
- No

If no, please explain.

This project will use an existing database server but requires new web application server and network components.

4.27. 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:

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

BFS applied for and was awarded a federal grant to fund this project. If the project does not proceed, funding will be lost and more EPAS devices will fail, reducing the efficiency and coverage of DUI testing and enforcement statewide.

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

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

Office of Traffic Safety (OTS) grant from October 1, 2008 through September 30, 2011

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

Fund Source	2009-10	2010-11	2011-12	2012-13	2013-14 and future	Total
General Fund						
Federal Fund						
Special Fund*						
Total						

* **Note:** Federal OTS grant used only by the DOJ.

Enterprise Architecture

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

Yes (The following is in draft and subject to revision)

No

DOJ Enterprise Architecture Principles

The following principles represent the criteria used to weigh potential investment and architectural decisions.

Principle #1 Business Drives Information Technology

Rationale

Information technology direction is driven by the business needs required to serve customers. Business events represent the essential activities that define the boundaries of a good information technology environment. Without knowing the business, the information technology infrastructure may be over- or under-built which can result in excessive technical complexity, cost and delays. This principle fosters an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to information technology changes. Technology changes provide an opportunity to improve the business process and hence, change business needs.

Implications

- Minimize unintended effects on business due to information technology changes.
- Build what we need, not what we want.
- Make it easier to identify technical impacts when business events change.
- Include the business and its perspective in the process.

Principle #2 Enterprise Focus

Rationale

Information management decisions will consider the impact and maximize the benefit to the agency as a whole. Decisions made from an agency-wide perspective have greater long-term value than decisions made from any particular departmental perspective.

Implications

- A governance structure must be implemented that will support agency-wide investment decision-making.
- Achieving maximum agency-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change.
- Some organizations may have to concede their own preferences for the greater benefit of the entire agency.
- Information management initiatives should be conducted in accordance with the agency-wide plan. Individual departments should pursue information management initiatives that conform to the blueprints and priorities established by the agency.

Enterprise Architecture

Principle #3 Common Business Solutions

Rationale

Development of common solutions used across the agency is preferred over the development of similar or duplicative solutions that are only provided to a particular program. Duplicative solutions are expensive and proliferate conflicting data.

Implications

- Departments will not be allowed to develop solutions for their own use that are similar or duplicative of an agency-wide solution. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Applications components should be shared across departmental boundaries.
- Changes to legislation and government code may be required to guide separate agencies to act in a unified manner.
- A common technology and organization infrastructure will be needed to support common business solutions.

Principle #4 Data is an Enterprise Asset

Rationale

The agency will coordinate interagency and intergovernmental data collection and management, to improve data sharing capabilities and reduce costs of acquiring and managing data. To enable the work of government, agencies need to combine data across systems; agencies need to share data with other agencies; users need to access information and services from varied sources; and businesses and government need to interface. Government work demands interoperability.

Implications

- Laws and statutes must be considered when sharing data across organizational boundaries.
- Data and information used to support agency-wide and statewide decision-making will be standardized to a much greater extent.
- Data standards and quality must be utilized across the enterprise.

Principle #5 Secure Enterprise Information

Rationale

Enterprise information will be secure from unauthorized access, modification, or destruction. Hacking, viruses, and terrorism increasingly threaten the state's systems. Government has a responsibility to maintain the public's trust in its systems from unauthorized access and to protect data integrity and confidentiality. Secure systems ensure the continuity of the state's business. Systems and data must be secured with security best practices and with security assessments being conducted on a regular basis.

Implications

- There will be a loss of public trust if not done correctly.
- Must be able to identify, publish, and keep applicable policies current.
- Security must enable, not impede, business.
- There must be preventive measures to secure systems; it is extremely costly to repair compromised systems.

Enterprise Architecture

- Security must be designed into systems from the beginning; it cannot be added later.
- Information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

Principle #6 Compliance with Agency-wide Standards

Rationale

Compliance with agency-wide standards will facilitate interoperability and consistency across solutions. Use of proven technology will simplify software design, reduce application development time, facilitate learning, improve systems maintenance and support, and promote information-sharing among organizations within the state, and thus reduce total cost of ownership.

Implications

- A process must be established for setting, reviewing and revising standards periodically, and granting exceptions. The process must be fast enough to support business and design drivers.
- Standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- Information technology policy and procedures must be tied directly to this principle.
- Fewer products and configurations simplify the information technology environment.

Principle #7 Compliance with Law

Rationale

Enterprise information management processes must comply with all relevant laws, policies, and regulations. Agency-wide policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

Implications

- The agency must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data.
- Changes in the law and changes in regulations may drive changes in our processes or applications.

Principle #8 Alignment with the State of California Enterprise Architecture

Rationale

Agency Enterprise Architecture components should be aligned (where possible) with state architectural standards and components in order to facilitate interoperability and consistency within the state's IT resources.

Implications

- The agency must be mindful of its obligation to leverage its IT resources (where required or needed) in combination with other state IT resources to the benefit of other governmental agencies and the public.
- Architectural consistency across state IT environments will facilitate increased effectiveness and efficiency within the state.

Enterprise Architecture

Principle #9 Alignment with Criminal Justice / Law Enforcement Architecture(s)

Rationale

Agency Enterprise Architecture components should be aligned (where possible) with criminal justice/law enforcement architectural standards and components in order to facilitate interoperability and consistency within the criminal justice/law enforcement IT resources.

Implications

- The agency must be mindful of its obligation to leverage its IT resources (where required or needed) in combination with other criminal justice/law enforcement resources to the benefit of the public.
- Architectural consistency across criminal justice/law enforcement IT environments will facilitate increased effectiveness and efficiency.

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		X		
Service		X		
Technical		X		
Data				X

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

Enterprise Architecture Governance Model

The governance structure being put in place for the development and maintenance of DOJ's enterprise architecture includes three organizational groups:

1. The Architecture Committee
 - a. Guide, review and approve/reject revisions to enterprise architecture models and standards
 - b. Promote enterprise architecture approaches
 - c. Chaired by CIO
 - d. Members include select managers/executives and subject matter experts (e.g. network, data, application, infrastructure, security, etc.) designated by the CIO in collaboration with agency executives

Enterprise Architecture

2. Architecture Model Coordination Teams
 - a. Guide, review and recommend model revisions for models within the scope of their team
 - b. Team 1: Business Reference & Service Reference Model Coordination Team
 - c. Team 2: Technical Reference Model Coordination Team
 - d. Team 3: Data References Model Coordination Team (to be added later)
 - e. Teams include line of business subject matter experts and technical subject matter experts
 - f. Teams leaders are designated by the CIO

3. Architecture Model Component Owners – individuals designated (in collaboration with the CIO and Architecture Model Coordination Teams) as responsible to maintain the currency of one or more architectural model components – owners will typically be people engaged in the use of architecture model component.

These three groups are the key element of the process flow for submission. Below are some sample scenarios of how these groups will facilitate the maintenance of the Enterprise Architecture at DOJ.

Scenario 1: Addition of a new architecture component

- Step 1: Idea germinates from within the organization
- Step 2: Statement of idea is submitted to appropriate Architecture Model Coordination Team
- Step 3: Architecture Model Coordination Team determines viability of idea
- Step 4: If idea is viable the Architecture Model Coordination Team in coordination with the CIO assigns an owner
- Step 5: The owner in collaboration with key stakeholders/experts prepares the new component and submits it to the Architecture Model Coordination Team
- Step 6: The Architecture Model Coordination Team reviews the new component, formulates a recommendation and forwards it to the Architecture Committee for approval/rejection
- Step 7: Upon approval by the Architecture Committee the new component is added to the online Architecture documentation and it becomes part of the architectural expectations of the agency

Scenario 2: Change of an existing architecture component

- Step 1: Need for change germinates from within the organization
- Step 2: Statement of change is submitted to appropriate Architecture Model Coordination Team
- Step 3: Architecture Model Coordination Team determines viability of change
- Step 4: If change is viable the Architecture Model Coordination Team in coordination with the CIO assigns an owner
- Step 5: The owner in collaboration with key stakeholders/experts prepares the component modification(s) and submits it to the Architecture Model Coordination Team
- Step 6: The Architecture Model Coordination Team reviews the change, formulates a recommendation and forwards it to the Architecture Committee for approval/rejection
- Step 7: Upon approval by the Architecture Committee the existing architectural component is the online Architecture documentation modified and the change becomes part of the architectural expectations of the agency

Enterprise Architecture

Scenario 3: Brainstorming new architectural approaches/ideas

Step 1: Brainstorming, ideas and suggestions are encouraged from any part of DOJ

Step 2: IT management and technology leaders in particular are expected to stay current with technology and business developments while continuously focusing on improving the enterprise architecture of DOJ.

Step 3: Managers and staff are encouraged either individually or in ADHOC groups to discuss, configure and propose new architectural approaches/ideas and submit them to the Architecture Model Coordination Teams

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

Yes

No

Name: _____

Classification: _____

Telephone Number: _____ **E-Mail:** _____

Information Security

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

The Information Security Officer (ISO) establishes department-wide standards and policies with participation from the Network Information Security Unit (NISU). NISU enforces policies and best practices through project development and other types of control implementations. The ISO is informed by NISU of proposed project development activities that may have an impact on the overall risk to the agency and its assets. The ISO proceeds with any necessary actions to be taken to mitigate any security issues with development efforts.

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?

The DOJ employs multiple data assets that fall under the jurisdiction and requirements of various regulations specific to protecting the confidentiality, integrity and availability of these assets. The DOJ has established a close alignment with industry best practices and requirements provided by the Federal National Institute and Standards and Technology (NIST) and Federal Information Process Standards (FIPS). The ISO and NISU enable these policies and standards throughout the department by implementing NIST/FIPS compliant security controls. NISU and the ISO continually analyzes risks to DOJ assets through security audits and develops security plans to effectively manage those risks to ensure continued compliance to the core principles, policies and standards established by the ISO.

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

- Yes
 No

The DOJ provides criminal history data to law enforcement agencies throughout California as one of our core services. Each law enforcement agency connecting to the DOJ is required to meet a minimum set of security standards based on FBI CJIS requirements, and signs a data exchange agreement. The DOJ also directly exchanges data with multiple criminal justice, medical, and public agencies. For these connections, the DOJ establishes mutual security standards based on the nature of the data being shared, enforced through interagency data exchange agreements.

If no, please explain.

- 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?

The ISO informs DOJ developers and programmers of any vulnerabilities or alerts pertaining to application and system development. NISU actively participates as security subject matter experts in Department web, application and system development projects and implementations. NISU and the ISO communicate Department security standards, policies and best security practices throughout the project lifecycle. Additionally, NISU, in collaboration with the ISO

Information Security

publishes software development best practice guidelines and prescriptive guidance for application developers on how to avoid common application security vulnerabilities in their application. NISU maintains application vulnerability scanning tools to test applications prior to production release. The ISO may perform independent security audits of DOJ applications and systems when necessary.

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: Andy Kraus

Classification: CEA I

Telephone Number: (916) 322-9036 **E-Mail:** Andy.Kraus@doj.ca.gov

Workforce Development, Workforce Planning and Succession Planning

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

- Yes
 No

If yes, briefly describe it.

The department workforce plans are not developed to the extent of those outlined in the OICO Succession Plan. However, the department has adopted several strategies regarding workforce needs. Current strategies include:

- mandatory completion of a department sponsored manager's academy for all IT supervisors and managers,
- participation by some IT managers in the statewide IT Managers' Academy,
- resource and skill assessment for each IT project undertaken,
- short-term consultant augmentation as needed to transition staff to new methods, processes and skill sets,
- formal training,
- use of retired annuitants for knowledge transfer, mentoring and training,
- inclusion of knowledge transfer as a specific activity and deliverable in all IT development contracts.

The department's IT organization is in the midst of a reorganization effort. Included in this effort is evaluation of roles and skills necessary to support legacy and new systems; project selection, management, monitoring and performance; IT architecture; IT security; and, IT development methods. The results of the role and skills assessment is expected to include some recommendation on workforce development.

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

If yes, briefly describe it.

See comments on C.1 above.

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

Workforce Development, Workforce Planning and Succession Planning

- Yes
- No

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
Assoc. Info Systems Analyst – Spec	49	21	Computer Operations Supvr I	6	3
Assoc. Programmer Analyst – Spec	25	13	Computer Operations Supvr II	3	2
Assoc. Systems Software Spec. – Tech.	8	1	Data Processing Manager I	1	0
Asst. Info. Systems Analyst	40	11	Data Processing Manager II	11	10
Computer Operations Spec. I	1	0	Data Processing Manager III	5	4
Computer Operations Spec. II	1	1	Data Processing Manager IV	2	2
Computer Operator	11	3	Information Systems Techn Supvr I	1	1
Information Systems Tech. Spec. I	1	1	Information Systems Techn Supvr II	3	3
Information Systems Tech. Spec. II	1	1	Sr Info Systems Analyst-Supvr	4	3
Information Systems Tech.	17	4	Sr Programmer Analyst-Supvr	4	3
Programmer I	1	0	Staff Info Systems	2	0

			Analyst-Supvr		
Programmer II	3	1	Systems Software Spec II-Supvry	3	0
Sr. Info. Systems Analyst – Spec.	9	4	Sytems Software Spec III-Supvry	2	1
Sr. Programmer Analyst – Spec.	20	10		0	0
Staff Info. Systems Analyst – Spec.	62	27		0	0
Staff Programmer Analyst – Spec.	30	18		0	0
Systems Software Spec. I – Tech.	17	7		0	0
Systems Software Spec. II – Tech.	3	0		0	0
Systems Software Spec. III – Tech.	2	1		0	0
Totals	301	124		47	32

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.

DOJ is in the process of moving from an informal alignment process to a more formal one. The more structured approach is being facilitated by the creation and implementation of a portfolio management framework managed under the umbrella of a newly established Project Management Office. With this additional focus and structure DOJ expects to enable better alignment of business and technology.

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)

Implementation is in the very early stages. The concept is defined, and the piloting of processes, methods and tools are just beginning.

- Planned or planning in progress
 Not implemented and not planned

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

DOJ is using Intuit's QuickBase, an online browser based toolset, as its platform for portfolio management.

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

- Implemented (Please describe)

DOJ is in the process of defining and implementing its second generation of a standard project management methodology. Key features/strategies of this second generation methodology include:

- More visibility and accessibility to project information
- Reusable project planning content
- Centralization of project information
- Value/results focused methods and approaches
- Varying requirements/standards based on size and priority of projects
- Streamlined approaches based on lessons learned (i.e. blending of state and vendor test teams)
- Balancing focus on the engineering and artistic sides of project management

Project Management, Portfolio Management and IT Governance

Implementation in progress (Please describe)

Planned or planning in progress

Not implemented and not planned

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

While certification is not a formal requirement, DOJ has worked to raise the level of its project management competency through training and mentoring. Project Managers have been given on-site consultant training and mentoring. This includes the Project Management training and certification program offered by U.C. Davis Extension. In the future our new Project Management Office will become a focal point for project competency. Our intent is to use the Project Management Office as the focal point for the development of strategies and resources to raise the level of project competency within DOJ.

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

The new Project Management office will have responsibility for development and maintenance of project management competency. In that regard, it is our intent to develop approaches and programs that include many of the items listed above.

Project Management, Portfolio Management and IT Governance

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

All projects are required to document the project governance practices in a Project Management Plan. Included in the plan are a Steering Committee framework, a communication management plan, a risk/issue management plan (that includes problem escalation and issue resolution), and a change management plan.

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

Yes (Please describe)

No

Each project is reminded and encouraged via independent oversight to conduct lessons learned exercises, minimally at the end of the project. For high criticality projects, a lessons learned is conducted at various stages throughout the project, and an Independent Project Oversight Consultant prepares a formal Lessons Learned document at the end of each fiscal year.