

Chapter 4800 - California Technology Agency

4800 STATE INFORMATION MANAGEMENT PRINCIPLES

(Revised 03/11)

The California Technology Agency (Technology Agency) has broad responsibility and authority to guide the application of information technology (IT) in California State Government. The Technology Agency's areas of responsibility include policy making, interagency coordination, IT budget and procurement review, technical assistance and advocacy. In view of the scope of these activities and their potential impact on state government, the Technology Agency has articulated the fundamental principles, policies and procedures to govern the use of information technology in Sections 4800 through 5180 of the State Administrative Manual (SAM).

Note that any and all project approvals or conditions made by the Technology Agency's predecessor organizations, the Office of the State Chief Information Officer (OCIO) prior to January 1, 2011, or the Department of Finance (Finance) prior to January 1, 2011, remain in effect unless otherwise notified.

Priority of Information Technology.

Information technology is an indispensable tool of modern government. Accordingly, each state agency is expected to seek opportunities to use this technology to increase the quality of the services it provides and reduce the overall cost of government.

Authority and Responsibility.

Each agency director should be knowledgeable about the information requirements and information management practices of the agency and should provide active leadership in the exploration of new opportunities to use information technology. Each agency should establish clear lines of authority and responsibility for information management.

Management of Information.

Each agency shall establish and maintain an information management function consistent with its own operational needs and organizational structure. This function shall serve to ensure the agency's ability to identify the information it collects, maintain the integrity and security of the information, and provide for appropriate access to the information.

Management Methods.

Each state agency shall employ proven management methodologies to guide and control the planning, acquisition, development, operation, maintenance, and evaluation of information management applications. Pilot projects and/or independent oversight shall be required for larger, more complex applications.

Basis for Decisions.

Decisions regarding the application of information technology shall be based on analysis of overall costs and benefits to the people of California over the life of the application. Each agency shall plan far enough into the future to ensure that adequate time is available for analysis of alternatives, for obtaining necessary management approvals, and for the administration of procurements. Agencies shall determine the impact of their decisions across departmental and agency lines and give priority to alternatives that provide the greatest benefit from a statewide perspective.

Record of Decisions.

Each agency shall maintain records of management decisions concerning the use of information technology. These records must be sufficiently detailed to satisfy the requirements of oversight agencies as well as internal management. The records must address such topics as:

1. Identification of information technology needs;
2. Setting of priorities for applications of information technology;
3. Evaluation of application alternatives;

4. Project management and control;
5. Contingency planning and risk management; and,
6. Operational controls and maintenance provisions.

Agency Personnel.

Agency managerial, technical, and user personnel should possess the knowledge and skills necessary to use information technology to the best advantage for the state. Each agency should regularly assess the information technology skills and knowledge of its personnel in relation to job requirements, identify and document training needs, and provide suitable training within the limits of available resources.

Compatibility.

In selecting or developing applications of information technology, each agency shall consider the benefits and costs of maintaining compatibility with other planned and existing applications within the agency and in other state agencies. Such consideration of compatibility shall include computer languages, applications and system software, computer hardware and telecommunications equipment, data formats, and the specific knowledge and skills required of state personnel.

Procurement.

In acquiring equipment, software, and services involving information technology, agencies shall seek maximum economic advantage to the state. Procurements shall normally be competitive, in conformance with the applicable sections of the Public Contract Code and SAM. Agencies shall use master contracts whenever the functional requirements for which the contract was awarded are substantially the same as the agency's requirements.

Cost Allocation.

Each agency shall adopt policies and establish procedures for assignment of costs associated with information technology by program or operational unit within the agency, as well as for the assignment and recovery of the costs of services provided to other agencies, private individuals, and organizations.

Risk Management. Each state agency shall adopt and maintain a risk management program for the purpose of identifying and avoiding or minimizing threats to the security of information it maintains and the operational integrity of its information systems, telecommunications systems, and data bases.

Documentation. Applications of information technology shall be fully documented with respect to the needs of (1) nontechnical users; (2) technical personnel; (3) agency measurement; and (4) outside auditors. The adequacy of documentation shall be an evaluation criterion in all procurements involving information technology (equipment, software, services and telecommunications facilities). Project plans shall include specific provision for the creation of suitable documentation.

Provision for Emergencies. In planning for the use of automated information systems and telecommunications facilities, agencies shall develop policies and procedures to be followed in times of emergency; when systems are preempted to preserve the public health, welfare or safety; and when other events occur which prevent reliance on automated systems for extended periods of time.

Individual Rights. Information management policies and procedures shall be consistent with the California Constitution, the Public Records Act, the Information Practices Act, and other applicable laws. Each state agency shall safeguard the right to privacy of individuals who are the subjects of the records it maintains.

Ethics. In the conduct of their operations and in the accomplishment of the policies stated above, state agencies and their employees shall employ information technology in a legal and ethical manner consistent with government statutes, rules and regulations. Information technology shall not be used for purposes that are unrelated to the agency's mission or that violate state or federal law. Contract provisions, including software licensing agreements, shall be strictly followed.

4804 ACCESS TO INFORMATION BY THE OFFICE OF THE LEGISLATIVE ANALYST
(Reviewed 03/11)

Section 11734 (f) of the Government Code requires that procedures be published in SAM to allow the Legislative Analyst to use data in, or products of, state data processing information systems to analyze

programs and budgets.

In order to enable the Legislature to determine the fiscal or program effects of changes (1) proposed by the Administration or (2) considered by the Legislature, any state department operating an automated information system shall, upon receiving a written request, allow the Legislative Analyst reasonable access to any relevant data contained in the system's master files, transaction files, history files and/or other appropriate automated files.

However, such access shall not be provided to information: (1) specifically prohibited by Federal law or (2) relating to proposed administrative actions (such as Budget Change Proposals submitted by individual state entities) not yet approved by the Administration.

It is the responsibility of the department to whom the information pertains to ensure that any data made available under these provisions are as accurate and up-to-date as is consistent with the department's normal use of data.

The Legislative Analyst must agree that any confidential information obtained under these provisions shall remain confidential.

4806 ACCESS TO INFORMATION BY THE CALIFORNIA STATE AUDITOR

(Reviewed 03/11)

Section 11734 (f) of the Government Code requires that procedures be published in SAM to allow the Auditor General in the conduct of his audit to use data in, or products of, state data processing information systems. Section 10527 of the Government Code provides that the Auditor General shall have access to, and authority to examine, records of any state agency. Section 10528 of the Government Code provides that the Auditor General shall examine and report annually upon the financial statements of the state and make special audits and investigations, including performance audits, of any state agency.

In order for the Auditor General to conduct these audits in an expeditious manner, any department operating a statewide information system shall, upon receiving a written request, allow the Auditor General "read only" access to any relevant data contained in the system's master files, transaction files, history files and/or other appropriate automated files.

The department operating the information system is authorized to require the Auditor General to reimburse it for any additional costs incurred as a direct result of the Auditor General's acquisition of data from the system.

It is the Auditor General's responsibility to check with the individual state entities to whom the information pertains to ensure that any data acquired under these provisions are accurate and up-to-date.

Any confidential information obtained by the Auditor General under these provisions shall remain confidential.

4810 STATUTORY PROVISIONS

(Revised 03/11)

The following provisions apply to all state departments, offices, boards, commissions, institutions, and special organizational entities except the State Compensation Insurance Fund, the Legislature, or the Legislative Data Center in the Legislative Counsel Bureau.

Office of the State Chief Information Officer:

Pursuant to Government Code Sections 11545 and 11546, the Secretary of California Technology is charged with the duty to advise the Governor on the strategic management and direction of the state's information technology resources. In addition to this advisory role, the Technology Agency is responsible for: establishing, maintaining, and enforcing the State's IT strategic plans, policies, standards procedures, and enterprise architecture; approval and oversight of IT projects; consulting with agencies during initial project planning; and suspending, reinstating, or terminating IT projects.

Department of Finance:

Pursuant to Government Code Section 11547, the Department of Finance shall perform fiscal oversight of the state's information technology projects. The oversight shall consist of a determination of the availability of project funding from appropriate sources and project consistency with state fiscal policy.

4815 AGENCY INFORMATION OFFICER AND DEPARTMENT CHIEF INFORMATION OFFICER RESPONSIBILITIES

(Revised 03/11)

Within the authority of Government Code (GC) Section 11545 and 11546, the Secretary of California Technology shall be responsible for providing technology direction to Agency Chief Information Officers (AIO) and department Chief Information Officers (CIOs):

1. Integrate statewide technology initiatives,
2. Ensure Agencies and Departments are in compliance with information technology and security policies and standards, and
3. Promote the alignment and effective management of information technology resources.

Agency Information Officers

All Agency Information Officers (AIOs) are responsible for overseeing the management of IT assets, projects, data systems, infrastructure, services and telecommunications through the oversight and management of department CIOs. Each AIO is responsible for developing an Agency Enterprise Architecture to rationalize, standardize and consolidate IT infrastructure, data, and procedures for all departments within their Agency.

Specific responsibilities for the AIOs are published in Information Technology Policy Letters or the Statewide Information Management Manual (SIMM) for new policies and initiatives. Each AIO must be compliant with the responsibilities as described in SAM, SIMM, and IT Policy Letters.

Department Chief Information Officers

Department CIOs are directly responsible for all IT activities within the department. CIOs are responsible for all IT systems, assets, projects, purchases, and contracts and will ensure department conformity with the Agency Enterprise Architecture. Department CIOs are also responsible for:

- Portfolio management of the department's technology initiatives.
- Operational oversight of IT functions, personnel and operations including:
 - Web application development;
 - Application and database management;
 - Security administration;
 - Telecommunications, including Public Safety Communications;
 - Project planning, consulting, and management; and
 - Help desk and customer service management.

Agency and department CIOs must be in compliance with state IT policies and procedures as described in SAM, SIMM and IT Policy Letters.

Non-Affiliated Chief Information Officers

With the exception of the responsibilities related to the oversight of Agency-affiliated department CIOs, non-affiliated department CIOs have the same responsibilities as AIOs. In addition, non-affiliated department CIOs also have the same responsibilities as Agency-affiliated department CIOs.

Reporting

Agency and Department CIOs are accountable to the Secretary of California Technology with respect to

technology direction, including, but not limited to, IT policy, planning and management.

All state employees in information technology classifications, and all other state employees or contractors performing IT activities and/or functions must be in a direct reporting relationship to the appropriate Agency or department CIO.

Consistent with the federated governance model, the Technology Agency will work with the Agencies and departments to implement this operating model in a way that aligns with their business operations.

4819 GENERAL

(Revised 09/02)

The SAM Section 4819 provides definitions and summarizes the compliance requirements for the administration of information technology in state government. Additional detail regarding specific requirements, policies or procedures is provided throughout SAM Sections 4800–5953, SAM Sections 6700 – 6780, and the State Information Management Manual (SIMM).

4819.2 DEFINITIONS

(Revised 03/12)

The following definitions of administrative and technical terms are provided to assist agencies in their application of information technology policy.

The primary source for technical definitions is the Information Processing Systems Technical Report, American National Dictionary for Information Processing Systems, developed by the American National Standards Committee, X3 Information Processing Systems. In some cases the definitions have been modified to meet state needs.

Agency: When used lower case (agency), refers to any office, department, board, bureau, commission or other organizational entity within state government. When capitalized (Agency), the term refers to one of the state's super agencies such as the State and Consumer Services Agency or the Health and Human Services Agency.

Baseline(d): An approved time phased plan for project work against which project execution is compared to measure and manage cost and schedule performance.

A project must be baselined in accordance with the milestones in the approved FSR. A project may not be re-baselined unless an approved SPR is available.

Cloud Computing: A Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Confidential Information: Information maintained by state agencies that are exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. See SAM Section 5320.5.

Continuing Costs: Costs associated with the operation and maintenance of an information technology system or application after development and implementation of the system.

Critical Application: An application that is so important to the state that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs. See SAM Section 4842.11.

Data: A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means.

Data Processing: The systematic performance of operations upon data, e.g., handling, merging, sorting, computing. Synonymous with information processing.

Data Processing System: A system, including computer systems and associated personnel, that performs input, processing, storage, output, and control functions to accomplish a sequence of operations on data.

Data/Information Storage: The retaining of data/information on any of a variety of mediums (i.e., magnetic disk, optical disk, or magnetic tape) from which the data can be retrieved.

Data Transmission: The conveying of data from one functional unit to one or more additional functional units through the transmission of signals by wire, radio, light beam, or any other electromagnetic means. (Voice or video transmissions are not considered data transmission for the purposes of state policy.)

Development: Activities or costs associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new information technology applications.

Electronic and Information Technology (EIT or E&IT): Includes information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information Kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines.

Emergency: A sudden, unexpected occurrence that poses a clear and imminent danger, requiring immediate action to prevent or mitigate the loss or impairment of life, health, property, or essential public services. SAM Section 6560, specifies that emergency expenditures cannot exceed \$25,000, unless approved by the Department of Finance.

Federated Data Center: A centralized Tier III-equivalent data center providing participating state departments the ability to operate their own environment with a degree of independence in the overall management of their server infrastructure. Federated Data Center (FDC) services will evolve to provide, at a minimum, shared network, storage, and backup infrastructures. Additionally, agencies can plan utilization of the FDC as a disaster recovery site.

Hardware: See IT equipment.

Information Processing: The systematic performance of operations upon data, e.g., handling, merging, sorting, computing. Synonymous with data processing.

Information Technology: Information technology means all computerized and auxiliary automated information handling, including systems design and analysis, conversion of data, computer programming, information storage and retrieval, voice, video, data communications, requisite systems controls, and simulation. The term "information technology" is commonly abbreviated as "IT".

Information Technology Activities: Any activity listed below, or any combination of these activities for a single information technology project, is to be considered an "information technology activity."

1. IT facility preparation, operation and maintenance.
2. Information management planning.
3. Feasibility determination, development and implementation of application systems or programs, or changes to application systems or programs to meet new or modified needs, or maintenance, including: feasibility study preparation, systems analysis, systems design, purchase and installation of software, programming, conversion of data or programs, documentation of systems and procedures, and project appraisal or assessment.
4. Operation of application systems or programs including handling, assembling, or editing of input-output data or media where information technology equipment or information technology personnel are used.
5. Services or equipment received through an EDP Master Agreement (SAM Section 5207.5).
6. Acquisition, installation, operation, and maintenance of data processing equipment.

7. Other installation management activities including performance measurement, system tuning, and capacity management.
8. Preparation and administration of requests for proposals or bid solicitations for contracts for any of the above activities.
9. Preparation of contracts, interagency agreements, and purchase estimates for any of the above activities.
10. Employment of personnel in support of, or directly related to, any of the above activities, including: administration, technical services, clerical services, travel, training, and preparation of periodic and special reports.
11. Control functions directly related to any of the above activities.

Information Technology Expenditure: The expenditure of funds regardless of source by any state entity for information technology activities, equipment, facilities, personnel, services, supplies and the automated processing of information.

Information Technology (IT) Project Oversight Framework: Minimum requirements for IT project management, risk management and IT project oversight activities for departments and agencies. Description of control agency project reporting requirements and processes for assessing department and agency project management and oversight activities. See SIMM Section 45.

Information Technology Procurement: Any contract, interagency agreement or purchase estimate to conduct any activity listed below, or any combination of these activities is to be considered an "information technology procurement."

1. IT facility preparation, operation maintenance.
2. Development and implementation of application systems or programs, or changes to application systems or programs to meet new or modified needs, or maintenance, including: feasibility study preparation, systems analysis, systems design, purchase and installation of software, programming, conversion of data or programs, documentation of systems and procedures, and project appraisal or assessment.
3. Operation of application systems or programs including handling, assembling, or editing of input-output data or media where information technology equipment or information technology personnel are used.
4. Services or equipment received through an EDP Master Agreement. SAM Section 5207.
5. Acquisition, installation, operation, and maintenance of data processing equipment.
6. Other installation management activities including performance measurement, system tuning, and capacity management.
7. Employment of personnel in support of, or directly related to, any of the above activities, including: administration, technical services, clerical services, travel, training, and preparation of periodic and special reports.
8. Control functions directly related to any of the above activities.

Information Technology Project: A project that encompasses computerized and auxiliary automated information handling, including systems design and analysis, conversion of data, computer programming, information storage and retrieval, data transmission, requisite system controls, and simulation, and related interaction between people and machines. Synonymous with IT project.

Input-Output Unit/Device: A unit or device in an IT system by which data may be entered into the system, received from the system, or both.

IT Equipment: Information Technology devices used in the processing of data electronically. The following are examples of IT equipment:

1. Central processing units (mainframes) and all related features and peripheral units, including processor storage, console devices, channel devices, etc.;
2. Minicomputers, midrange computers, microcomputers and personal computers and all peripheral units associated with such computers;

3. Special purpose systems including word processing, Magnetic Ink Character Recognition (MICR), Optical Character Recognition (OCR), photo composition, typesetting and electronic bookkeeping;
4. Communication devices used for transmission of data such as: modems, data sets, multiplexors, concentrators, routers, switches, local area networks, private branch exchanges, network control equipment, or microwave or satellite communications systems; and
5. Input-output (peripheral) units (off-line or on-line) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, computer output to microform converters (COM), video display units, data entry devices, teletypes, teleprinters, plotters, scanners, or any device used as a terminal to a computer and control units for these devices.

IT Personnel: All state personnel employed in IT or telecommunications classifications as defined by the Department of Personnel Administration or by the Trustees of the California State University and Colleges, and all personnel of other classifications in state agencies who perform information technology activities for at least 50 percent of their time. Users of personal computers and office automation are not included in this category unless they are in information technology classifications or spend at least 50 percent of their time performing information technology activities.

IT Supplies: All consumable items and necessities (excluding equipment defined as IT equipment) to support information technology activities and IT personnel, including:

1. Documents (such as standards and procedures manuals, vendor-supplied systems documentation, and educational or training manuals);
2. Equipment supplies (such as printer forms, punch card stock, disk packs, "floppy" disks, magnetic tape, and printer ribbons or cartridges); and
3. Furniture (such as terminal tables and printer stands).

Life Cycle: The anticipated length of time that the information technology system or application can be expected to be efficient, cost-effective and continue to meet the agency's programmatic requirements. Synonymous with operational life system.

Maintenance: Activities or costs associated with the ONGOING UPKEEP of operational applications of information technology. Maintenance includes correcting flaws, optimizing existing systems or applications, responding to minor changes in specified user requirements, renewal of equipment maintenance agreements, and meeting normal workload increases using substantially the same equipment, facilities, personnel, supplies and software.

Mobile Web: Mobile Web refers to browser-based access to the Internet or Web applications using a mobile device, such as a smart phone, connected to a wireless network.

Network Equipment: Equipment facilitating the use of a computer network. This includes routers, switches, hubs, gateways, access points, network bridges, modems, firewalls, and other related hardware and software.

One-Time Costs: Costs associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new information technology applications. See State Information Management Manual (SIMM) Section 20 (Economic Analysis Workbook Package).

Open Source Software: Software that includes distribution terms that comply with the following criteria provided by the Open Source Initiative: *(The open source definition used here is from the Open Source Initiative and is licensed under a Creative Commons Attribution 2.5 License* (<http://creativecommons.org/licenses/by/2.5/>)

1. Free Redistribution: The software can be given as part of a package with other applications;
2. Source Code: The code must either be distributed with the software or easily accessible;
3. Derived Works: The code can be altered and distributed by the new author under the same license conditions as the product on which it is based;

4. Integrity of the author's source code: Derived works must not interfere with the original author's intent or work;
5. No discrimination against persons or groups;
6. No discrimination against fields of endeavor: Distributed software cannot be restricted in who can use it based on their intent;
7. Distribution of license: The rights of the program must apply to all to whom the program is re-distributed without need for an additional license;
8. License must not be specific to a product; Meaning that an operating system product cannot be restricted to be free only if used with another specific product;
9. License must not contaminate other software; and
10. License must be technology-neutral.

Operational Life: See life cycle.

Operations: Activities or costs associated with the CONTINUED USE of applications of information technology. Operations includes personnel associated with computer operations, including network operations, job control, scheduling, key entry, and the costs of computer time or other resources for processing.

Peripheral Unit/Device: With respect to a particular processing unit or device, any equipment that can communicate directly with that unit or device.

Power Management: A feature of some electrical appliances, especially copiers, computers and computer peripherals such as monitors and printers, which turns off the power or switches the system to a low-power state when inactive.

Previously Approved Effort/Project: An information technology activity or project previously approved by the Technology Agency (or the Office of the State Chief Information Officer (OCIO) prior to January 1, 2011, or Finance prior to January 1, 2008) or the agency's executive officer in accordance with SAM Section 4819.3. Qualification of an activity as a previously approved effort requires an approved Feasibility Study Report (FSR) AND an approved Post-Implementation Evaluation Report. Applicable activities include meeting modified needs, improving the effectiveness of the activity, program or system maintenance, or extension of existing services to new or additional users performing essentially the same functions as those that the project was designed to support. A previously approved effort/project must use substantially the same equipment, facilities, technical personnel, supplies and software to meet substantially the same requirements or to meet normal workload increases. (Note: "Substantially the same equipment" does not include the addition, upgrade or replacement of a central processing unit.)

Program: A sequence of instructions suitable for processing. See information processing or data processing.

Programming: The designing, writing, testing, debugging, and documentation of programs.

Project: A set of related activities carried out according to a plan and budget to achieve a specific set of objectives within a specified time schedule. (See information technology project.)

Project Oversight: An *independent* review and analysis to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies any issues and risks affecting these project components.

Proprietary Software: Computer programs which are the legal property of one party, the use of which is made available to a second or more parties, usually under contract or licensing agreement.

Public Facing Applications: Any web-facing application designed and delivered with the intent of access by individuals or organizations over the public internet. Public facing applications are exposed to the broadest base of potential users (e.g. citizens), and are accessed via a web-browser.

Public Information: Any information prepared, owned, used or retained by a state agency and not

specifically exempted from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6270) or other applicable state or federal laws.

Sensitive Information: Information maintained by state agencies that require special precautions to protect it from unauthorized modification or deletion. See SAM Section 5320.5. Sensitive information may be either public or confidential (as defined above).

Server Room: Any space that houses computer operations. Such computer operations could utilize mainframes, servers, or any computer resource functioning as a server.

Shutdown: Turning the power off in a controlled manner.

Software: Programs, procedures, rules, and any associated documentation pertaining to the operation of a system. (Contrast with hardware.)

Statewide Information Management Manual (SIMM): The Statewide Information Management Manual (SIMM) as structured by the Technology Agency contains instructions and guidelines as well as samples, models, forms and communication documents that state agencies either must use, or will find helpful to use, in complying with established state policy relating to IT. For clarity, references in SIMM to "Department of Finance" that are not related to budget documents such as Budget Change Proposals or Finance Letters, should be read as references to the "California Technology Agency".

System Standby: A low power mode for electronic devices such as computers, televisions, and remote controlled devices (aka "sleep mode"). These modes save significant electrical consumption compared to leaving a device fully on and idle but allow the user to avoid having to reset programming codes or wait for a machine to reboot.

Technology Letter: Letters issued by the Technology Agency conveying official communications regarding state information technology (IT), announcing new (or changes to existing) IT policies and procedures, or announcing new (or changes to existing) state IT services or standards.

Telecommunications: Includes voice and data communications, the transmission or reception of signals, writing, sounds, or intelligence of any nature by wire, radio, light beam, or any other electromagnetic means.

Tier III-Equivalent Data Center: Data Center facility consisting of multiple active power and cooling distribution paths; however, only one path is active. The facility has redundant components and is concurrently maintainable providing 99.982% availability.

Validation: The process of evaluating software during or at the end of the development process to determine whether it satisfies specified requirements. [IEEE-STD-610]

Verification: The process of evaluating software to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. [IEEE-STD-610]

Virtualization: A framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others.

Workload Increase: Employing substantially the same resources (equipment, facilities, personnel, supplies, software) to process a greater volume of the same or similar information. The results of the processing are the same or similar outputs distributed to comparable users.

4819.3 STATE INFORMATION MANAGEMENT AUTHORITY AND RESPONSIBILITY

(Revised 03/11)

Pursuant to Government Code Sections 11545 and 11546, the Secretary of California Technology is charged with the duty to advise the Governor on the strategic management and direction of the state's information technology resources. In addition to this advisory role, the Technology Agency is responsible for: establishing, maintaining, and enforcing the State's IT strategic plans, policies, standards procedures, and enterprise architecture; approval and oversight of IT projects; consulting with agencies during initial project planning; and suspending, reinstating, or terminating IT projects.

4819.31 BASIC POLICY

(Revised 06/11)

Each state agency is required to:

1. Establish and maintain a Disaster Recovery Plan, so that it will be able to protect its information assets in the event of a disaster or serious disruption to its operations, and submit the plan or its update to the Office of Information Security (OIS) as outlined in the Disaster Recovery Plan Quarterly Reporting Schedule (SIMM Section 05). See SAM Sections 5350-5355.
2. Establish an ongoing information management strategic planning process to support the accomplishment of its overall business strategy (i.e., its strategy to carry out its programmatic mission) and submit its strategic plan to the Technology Agency for approval. See SAM Section 4900.2.
3. Adopt standards for an agency information technology infrastructure consistent with SAM Section 4900.1.
4. Prepare annually an IT Capital Plan for long-term planning of the State's strategic IT investments. See SAM Section 4904.
5. Use the California Project Management Methodology (CA-PMM) as described in SAM Section 4910 for managing all IT projects.
6. Implement their Enterprise Architecture in accordance with the guidelines and instructions included in SIMM Section 58.
7. Conduct a feasibility study in order to establish the business case for each proposed information technology project (development or acquisition) and obtain approval of the FSR from the Technology Agency, or, if approval authority has been delegated to the agency director, from the agency director before expending any resources on the project. See SAM Sections 4819.34-4819.35.
8. Complete and sign the Service Contract Information Technology (SCIT) Certification for each proposed non-IT service contract and service contract amendment, including non-competitive bids. Please note that IT goods and services, including contracts associated with a Feasibility Study Report (FSR) or FSR Reporting Exemption Request approved by the Technology Agency, would be procured using one of the IT contracting processes developed expressly for IT. In these cases, completion of the SCIT is not necessary, since IT procurements are already subject to Technology Agency review and oversight requirements. The SCIT Certification is available in SIMM Section 16A, and includes instructions for completing and submitting the SCIT Certification.
9. Submit all Formal IT Solicitations, (as defined in the State Contracting Manual (SCM), Volume 3, Chapter 4, Section B1.0) to the Technology Agency for review prior to release to the public. Review of Informal IT Solicitations is delegated to departments. The following materials shall be included with the Formal IT Solicitation package:
 - a. A completed and signed *Formal Information Technology Solicitation Executive Approval Transmittal*, which is available in SIMM Section 28A.
 - b. All sections, appendices, attachments and exhibits comprising the Formal IT Solicitation.
 - c. The Information Technology Procurement Plan prepared in accordance with Volume 3, Chapter 2, Section B3 of the SCM and approved by the DGS or, for Formal IT Solicitations delegated by the DGS in accordance with SAM section 5200.5, approved by the department.

Review of Formal IT Solicitations is in addition to existing IT-related reporting and approval requirements. The instructions and time frame for submitting Formal IT Solicitations to the Technology Agency for review is specified in SIMM Section 05A.

For addenda focusing on Technical or Functional Requirements within the solicitation that are specific to the California IT Strategic Plan, alignment with the Statewide Enterprise Architecture, or

alignment with IT reporting and approval requirements, the Technology Agency will collaborate with the DGS Procurement Division (PD), for DGS-Administered Procurements, and with the issuing department, for delegated procurements, prior to release. All other addenda will be reviewed by the DGS PD or the issuing department, as appropriate. The time frame for submitting addenda will be determined in collaboration with the Technology Agency and the DGS PD or with the issuing department as appropriate.

Departments shall not be relieved of responsibility for major scope deviations within the Formal IT Solicitations or addenda reviewed by the Technology Agency unless:

- a. The department has specifically informed the Technology Agency-Program Management Office (PMO) in writing of such major scope deviations at the time of submittal; and
 - b. The Technology Agency-OTech has given written approval of the specific deviation.
10. Manage information technology projects following the established IT Project Oversight Framework (SIMM Section 45) minimum requirements, to ensure that projects are completed on-time, within budget, and that they accomplish the objectives defined in their FSRs. See SAM Section 4800.
 11. Protect the integrity of its information management capabilities and databases and ensure the security and confidentiality of information it maintains.
 12. Establish an ongoing acquisition planning process to develop IT Procurement Plans (ITPP) for IT project acquisition of IT goods and services as determined by the Department of General Services.
 13. Agencies shall implement power management practices on all desktop and laptop computing devices, thin client devices, printers, copiers, scanners, and monitors. During hours of normal operation, devices which are not in use for 30 minutes shall automatically go into an energy-saving mode. Devices shall be shutdown at the end of the normal business day.

In addition, agencies shall fully implement power management software for desktop and laptop devices by December 31, 2010, or six months after the 2010-11 Budget has been enacted, whichever is later. Agencies shall also implement standby and shutdown practices for all devices within the scope of this policy beginning December 31, 2010.

Exemptions must be approved in writing by the Agency Chief Information Officer (Agency CIO) or the department's Chief Information Officer (CIO). Exemptions are limited to:

- Devices which remain in active mode to meet State operational needs. An example of a valid exemption would be a desktop computer and monitor utilized to manage batch programs 24 hours per day, seven days per week.
- Facilities with electrical service bundled-in with facility lease contracts where state entities would not likely receive offsetting benefits from acquired power management software. In this instance, compliance can be achieved through the use of standard operating systems functionality (e.g., Windows).

If an agency fails to meet these requirements, the agency will be required to obtain Technology Agency approval before expending any resources on information technology projects.

The project approval process is described in SAM Section 4819.34.

4819.32 EXCLUSIONS

(Revised 03/11)

For purposes of the IT Project Submittal and Approval Policy, the following are excluded from State Administrative Manual (SAM) Section 4819.3, which defines State information management authority and responsibility for IT projects:

1. The SAM Section 4819.3 shall apply to all State departments, offices, boards, commissions, institutions, and special organizational entities except the State Compensation Insurance Fund, the Legislature, or the Legislative Data Center in the Legislative Counsel Bureau.
2. Information technology activities directly associated with single-function process-control systems (such as those applied in the controlling of water gates, traffic signals, or environmental systems for buildings), analog data collection devices, or telemetry systems are excluded from SAM Section 4819.3. Process Control, for the purposes of the exclusions from Technology Agency project approval and oversight, includes automated processing systems that monitor and control the operation of a single function system, and that can perform that control in isolation from other systems. Examples may include all components necessary to monitor and control the traffic lights at an intersection, the position of water restriction and diversion components in a water supply and distribution system, or to adjust the behavior of a motorized conveyer in response to changes in load and demand.

Sensors, telemetry devices, functional components such as motors or traffic lights, electronic control processors, and the network system that connects those devices into a single-function process control system meet the process control system exclusion.

Process control should not be interpreted to include information processing and network systems in which data is gathered, stored, transmitted, processed, analyzed, displayed, printed or reported for purposes other than the direct, automatic monitoring and controlling of a single function system, or for the manual review of the performance and activities of that single system.

Any component that may be added to any process control system, such as additional sensors, processing capacity or network communications capability, that is necessary for use in conjunction with a current or planned information technology system must be included in all feasibility study reports, plans, proposals and budget estimates for the information technology system.

3. Acquisition of telecommunications equipment used exclusively for voice or video communications are excluded from SAM Section 4819.3. This exclusion does not apply to:
 - a. Voice systems that include the use of interactive databases.
 - b. Videoconferencing systems that include the transmission of sensitive data or the use of interactive databases.
4. Acquisition of electronic typewriters and copiers are excluded if they are NOT:
 - a. Capable of general purpose computing; or
 - b. Intended to be used as an input/output peripheral device to a computer system.
5. Acquisition of the following consumable items or office equipment necessary to support approved information technology activities and personnel are excluded
 - a. Documents (such as standards and procedures manuals, vendor-supplied systems documentation, and educational training manuals);
 - b. Equipment supplies (such as printer forms, disk packs, "floppy" disks, compact disks, magnetic tape, and printer ribbons or cartridges); and,
 - c. Furniture (such as terminal tables and printer stands).

4819.34 PROJECT APPROVAL AUTHORITY

(Revised 03/11)

Authority for approval of information technology projects lies with the Technology Agency, but it is the intention of the State's Chief Information Officer to delegate approval authority to agency directors to the maximum extent practicable. When an agency's proposed expenditures on information technology are consistent with established policies and when the agency has consistently adhered to those policies and successfully implemented information technology projects, the Technology Agency will consider delegating authority for the

approval of resources to agency directors, as defined below.

The Technology Agency will establish an agency-specific cost delegation level, i.e., the project cost level above which the agency must obtain the Technology Agency's approval of an FSR or Feasibility Study Report - Reporting Exemption Request (FSR-RER) (see SAM Section 4819.37) before the agency is authorized to initiate the project.

The Technology Agency's delegations fall into one of three general groups:

Group 1 - Desktop and Mobile Computing Delegations—Agencies that have established and currently maintain an acceptable operational recovery plan and plan for the appropriate application of desktop and mobile computing will be delegated authority for the acquisition of equipment and software to support their desktop and mobile computing activities. See SAM Section 4989.2.

Group 2 - Agency Delegation for Non-Reportable Projects—Approval authority for projects which are not classified as reportable is delegated to the agency director. Agencies undertaking delegated projects are expected to employ appropriate project review, approval, and reporting procedures as specified in SAM Sections 4819.35 and 4819.36. See SAM Sections 4819.37 and 4819.39 for a list of reportable project criteria and a definition of delegated cost threshold.

Group 3 - Requested Delegation for Reportable Projects—An agency with an acceptable Disaster Recovery Plan and an Agency Information Management Strategy that has been approved by the Technology Agency may submit a Feasibility Study Report - Reporting Exemption Request (see SAM Section 4819.38) to the Technology Agency prior to the encumbrance or expenditure of funds, including the use of staff resources, on the project beyond the feasibility study stage. The Technology Agency will review the form and notify the agency whether it has been delegated approval authority for the proposed project. If delegation is not granted, the agency must submit the project FSR to the Technology Agency for approval.

1. Among the factors considered by the Technology Agency in determining whether a project should be delegated are:

- a. The apparent adequacy of the agency's planning process;
- b. The cost, scope, and complexity of the project;
- c. The size and composition of project staff;
- d. The agency executive staff's project management experience;
- e. The level of complexity and completeness of prior FSRs prepared by the agency;
- f. The number and complexity of previous information technology projects attempted by the agency;
- g. The demonstrated ability of agency project management staff to successfully monitor, control, and report progress during a complex undertaking; and
- h. The agency's past success in applying information technology to attain goals on time and within budget and to realize expected objectives.

Delegation of approval authority will NOT normally be given for projects which:

- a. Have significant statewide, interdepartmental, or intergovernmental impact;
- b. Involve the establishment or use of nonstandard or extensive communication facilities;
- c. Propose software or equipment acquisition expenditures that are large in relation to the agency's information technology budget;
- d. Have the potential for involving new or unfamiliar technology;

- e. Produce revenue for the state, such as licensing fees, tax collection, etc.;
 - f. Have a high potential risk associated with the security and confidentiality of the information being processed; or
 - g. Depend upon decisions to be made during the development or enactment of the Governor's Budget, such as approval of a Budget Change Proposal or Budget Revision.
2. Splitting a project into smaller projects to avoid either fiscal or procedural controls is prohibited.
 3. Agencies undertaking delegated projects are expected to employ appropriate project review, approval, and reporting procedures as specified in SAM Sections 4819.35 (Feasibility Study Report) and 4819.36 (Project Reporting/Oversight) below.
 4. All information technology projects are subject to audit. Documentation supporting project decisions must be kept by the agency for a minimum of two years following approval of the Post-Implementation Evaluation Report (PIER). See SAM Sections 4947-4947.2.
 5. The Technology Agency, at its discretion, may rescind previously delegated approval authority for individual projects or for all information technology activities in progress or proposed by an agency. The Technology Agency may require that project planning, design or implementation be halted or redirected.

The decision to rescind delegation will typically be based on review (audit) of the agency's information management practices; review of a specific project; redefinition of the project; significant increases in project cost projections; major cost overruns; specific control language placed on expenditures through legislation (i.e., the Budget Act); identification of significant unresolved technical issues; or a change in the direction of state policy.

4819.35 FEASIBILITY STUDY REPORT

(Revised 03/11)

1. The mechanism for approving information technology projects is the Feasibility Study Report (FSR). The FSR establishes the business case for investment of state resources in the project by setting out the reasons for undertaking the project and analyzing its costs and benefits.
2. An FSR, prepared in accordance with SAM Section 4928, must be approved for every information technology project prior to the encumbrance or expenditure of funds on the project, including the use of staff resources, beyond the feasibility study stage. The only exceptions to this requirement is that the feasibility studies for projects whose costs fall below a specified level may be documented by means of a Project Summary Package (see SAM Section 4930 and SIMM Section 20). Agencies are required to follow the SIMM Section 20 instructions for preparing and submitting the FSR.
3. If, during project development or implementation, the agency finds that program requirements cannot be adequately satisfied by the course of action described in the approved FSR and that an alternative course of action is more appropriate, a Special Project Report (SPR) (SAM Sections 4945-4945.2 and SIMM Section 30) shall be prepared. No encumbrance or expenditure of funds, including the use of staff resources, shall be made to implement such change or alternative course of action until approval has been received from the Technology Agency, or from the agency director if the Technology Agency has delegated approval of the project to the director and the project remains within the limitations of the agency's delegated authority. SPRs that must be submitted to the Technology Agency must be transmitted within 30 days after recognition of the situation that necessitates preparation of the SPR. Agencies are required to follow the SIMM Section 30 instructions for preparing and submitting the SPR.

4. Projects subject to approval by the Technology Agency (non-delegated projects) require submission of an FSR to the Technology Agency and to the Office of the Legislative Analyst. In addition, the FSR must be submitted to the Department of General Services when the contract total exceeds the agency's delegated purchasing authority. See SIMM Section 20.
 5. The DGS is responsible for policies and processes for IT procurement. For projects reportable to the Technology Agency, state agencies must submit FSRs that include the proposed IT procurement strategy. Prior to submission of the FSR for the Technology Agency's review, state agencies must consult with DGS Procurement Division to ensure project alignment with current procurement guidelines on all IT procurement exceeding \$500,000 or for all IT procurements if the agency does not hold a DGS Procurement Division IT procurement delegation.
 6. Projects whose approval has been delegated to the agency director normally require an FSR prepared in accordance with SAM Section 4928 and approval of the FSR by the agency director (SAM Sections 4921 and 4926). A copy of the report, including the Project Summary Package, and a signed document indicating approval by the agency director must be on file in the agency.
 7. The Technology Agency may decide to review specifications in procurement documents before they are advertised to ensure that the specifications are consistent with the functional specifications and system design in the FSR or SPR for the projects. See SAM Section 5211.1.
-

4819.36 PROJECT REPORTING/OVERSIGHT

(Revised 03/11)

1. **Projects Approved By the Technology Agency**—Project reporting documentation submitted to the Technology Agency usually will require:
 - a. Submission of an SPR (SAM Sections 4945-4945.2) to the Technology Agency and the Office of the Legislative Analyst, if:
 1. The total information technology project costs deviate or are anticipated to deviate by ten percent (higher or lower) or more, or by more than a specifically designated amount as determined by the Technology Agency, from the last approved estimated information technology project budget (to be measured against the combined total of each fiscal year's One-time Project Costs plus Continuing Project Costs);
 2. The last approved overall project development schedule falls behind or is anticipated to fall behind by ten percent or more;
 3. The total program benefits deviate or are anticipated to deviate by ten percent (higher or lower) or more from the last approved estimated total program benefits (to be measured against the combined total of each fiscal year's Cost Savings and Cost Avoidances);
 4. A major change occurs in project requirements or methodology;
 5. Any conditions occur that require reporting to the Technology Agency as previously imposed by the Technology Agency; or
 6. A significant change in state policy draws into question the assumptions underlying the project.
 - b. Submission of the Independent Project Oversight Report (IPOR), (see SIMM Section 45, Appendix G), on a monthly basis for projects classified by the Technology Agency as high criticality projects and on a quarterly basis for projects classified as medium criticality. The Technology Agency may modify the IPOR reporting frequency based on project performance. The Technology Agency may also validate the content of the IPORs for reportable projects as needed.
 - c. Submission of a Project Status Report (PSR), (see SIMM Section 17A and 17D.2) on a monthly basis for projects classified by the Technology Agency as high criticality, quarterly for medium criticality, and semi-annually for low criticality projects unless the Technology Agency has

specified a more frequent reporting period. Please see SIMM Section 05A for the PSR submittal schedule.

- d. Submission of a baselined and current Microsoft Project schedule with the submission of each PSR.
- e. Submission of a Post-Implementation Evaluation Report (PIER) (SAM Sections 4947-4947.2) to the Technology Agency and the Office of the Legislative Analyst at the conclusion of the project.
- f. The Technology Agency **MAY** require submission of specific project reports (SAM Section 4944) to the Technology Agency and the Office of the Legislative Analyst.

The Technology Agency may require agencies to submit an SPR under other circumstances, such as the agency's failure to meet a critical milestone or a significant increase in the project's cost in any fiscal year relative to the costs that were forecast when the project was approved by the Technology Agency. Additionally, the Technology Agency may require periodic reviews be conducted at any point during the project.

2. **Projects Approved By The Agency Director**—Projects for which reporting was delegated to the agency director require at a minimum:

- a. Appropriate project oversight and project reporting to the agency director in lieu of the Technology Agency, and maintenance of documentation in support of agency decisions on the project. Documentation should be sufficient to meet the needs of outside auditors and to prepare the PIER.
- b. Approval of a PIER (SAM Sections 4947-4947.2) by the agency director at the conclusion of the project.
- c. Submission of a SPR (SAM Sections 4945-4945.2) to the Technology Agency and the Office of Legislative Analyst if:
 1. Any criteria listed in SAM Section 4819.37, other than the project's cost exceeding the level the Technology Agency may have delegated to the agency, arise during the development or implementation of the project;
 2. A significant change in state policy draws into question the assumptions underlying the project; or
 3. The project costs exceed or are estimated to exceed the cost Technology Agency may have delegated to the agency AND one or more of the following conditions are true:
 - a. The total information technology project costs deviate or are anticipated to deviate by ten percent (higher or lower) or more from the estimated information technology project budget (to be measured against the combined total of each fiscal year's One-time Costs plus Continuing Costs);
 - b. The overall project development schedule falls behind or is anticipated to fall behind by ten percent or more;
 - c. The total program benefits deviate or are anticipated to deviate by ten percent (higher or lower) or more from the estimated total program benefits (*to be measured against the combined total of each fiscal year's Cost Savings and Cost Avoidances*); or
 - d. A major change occurs in project requirements or methodology.

Based on its review of the Agency Information Management Strategy (see SAM Sections 4900-4900.6) and its assessment of the agency's project management capabilities, the Technology Agency **MAY** require one or more of the following additional project reporting/oversight responsibilities for projects subject to oversight by the agency director:

1. Submission of the FSR and/or approval document, signed by the agency director, to the Technology Agency and the Office of the Legislative Analyst.
2. Submission to the Technology Agency of a detailed project schedule showing key milestones during the life of the project;
3. Submission of periodic project reports (SAM Section 4944) or SPRs (SAM Sections 4945-4945.2) to the Technology Agency and the Office of the Legislative Analyst; or
4. Submission of a PIER (SAM Sections 4947-4947.2) to the Technology Agency and the Office of the Legislative Analyst at the conclusion of the project.

Responsibilities and Tasks

California Technology Agency

1. The Technology Agency is responsible for developing and maintaining the state-level IT Project Oversight Framework (see SIMM Section 45), which provides the minimum requirements for IT project management, risk management, project oversight, and project reporting activities at the department, agency and control agency levels.
2. The Technology Agency is responsible for assessing department and agency IT project management and oversight activities to ensure compliance with state-level IT policies and standards. The Technology Agency will assess IT projects to determine the degree to which projects are on costs, schedule, and scope as compared to the approved project plan.
3. The Technology Agency will recommend and pursue prescriptive measures and corrective actions to minimize risk to the state and help ensure that IT projects achieve expected outcomes in accordance with the approved project plan.

Agencies

1. Agencies are responsible for developing IT strategic plans that are aligned with their business plans and ensuring that IT plans are updated as their business needs and requirements change.
2. Agencies have ultimate responsibility and accountability for the successful implementation of their IT initiatives and must implement processes and procedures to facilitate success, including appropriate project management and quality assurance processes and methodologies.
3. Agencies are responsible for establishing the required project management and oversight activities and functions defined in the IT Project Oversight Framework (see SIMM Section 45). Each agency must update its project management and oversight practices to reflect changes in State policy, processes, and the IT Project Oversight Framework.
4. Agencies are responsible for ensuring that projects consistently follow state-level IT oversight policies and requirements, legislative mandates, and applicable laws.
5. Agencies are responsible for providing project status information sufficient to allow the Technology Agency to meet its oversight reporting and full disclosure responsibilities.

4819.37 PROJECT REPORTING CRITERIA (Revised 03/11)

Before encumbering or expending funds on, or dedicating staff resources to, any of the following reportable projects, the agency must: (1) obtain the Technology Agency's approval of an FSR for the project; or (2) obtain the Technology Agency's approval of a Feasibility Study Report - Reporting Exemption Request (FSR-RER), with the subsequent approval of an FSR by the agency director:

1. Projects whose initiation depends upon decisions to be made during the development or enactment of the Governor's Budget, such as approval of Budget Change Proposal or Budget Revision to increase

the agency's existing information technology activities related to the project;

2. Projects that involve a new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation;
3. Projects that have a cost that exceeds the level the Technology Agency may have delegated to the agency and do not meet the criteria of a desktop and mobile computing commodity expenditure (see SAM Section 4989-4989.3);
4. Projects that meet previously imposed conditions by the Technology Agency.

Agencies that seek exemption from project reporting to the Technology Agency for a project meeting any of the above criteria must submit an FSR-RER (see SAM Section 4819.38) to the Technology Agency. An agency with an acceptable Disaster Recovery Plan and an Agency Information Management Strategy that has been approved by the Technology Agency may submit an FSR-RER.

4819.38 PREPARING THE FEASIBILITY STUDY REPORT - REPORTING EXEMPTION REQUEST (Revised 06/04)

SIMM, Section 40 provides instructions for completing the Feasibility Study Report - Reporting Exemption Request (FSR-RER). Agencies are required to follow the SIMM instructions for preparing and submitting the FSR-RER.

4819.39 DELEGATED COST THRESHOLD (Revised 03/11)

The Technology Agency assigns each agency a minimum total project development cost threshold for reporting purposes. See SIMM Section 15. The Technology Agency delegates to the agency the resource approval authority for any IT proposal with an estimated total development cost equal to or less than the agency's assigned cost threshold, provided the proposal does not meet any other Technology Agency established reporting criteria defined in Section 4819.37.

The total development cost is synonymous with one-time cost and is defined as all estimated or projected costs associated with the analysis, design, programming, verification and validation services, staff training, data conversion, acquisition, and implementation of an information technology investment. Excluded from development costs are estimated costs of continued operations and maintenance.

4819.40 EXPENDITURES FOR ONGOING INFORMATION TECHNOLOGY ACTIVITIES (Revised 03/11)

Expenditures in support of an ongoing information technology activity will normally not require the Technology Agency approval of a new FSR providing:

The activity meets the definition of previously approved project/effort as defined in SAM Section 4819.2:

Applicable activities include meeting modified needs, improving the effectiveness of the activity, program or system maintenance, or extension of existing services to new or additional users performing essentially the same functions as those that the project was designated to support. A previously approved effort/project must use substantially the same equipment, facilities, technical personnel, supplies and software to meet substantially the same requirements or to meet normal workload increases.

Note:

1. "Substantially the same equipment" does not include the addition, upgrade or replacement of a central processing unit (mainframe).
2. Minor changes in functionality and/or equipment will normally meet the definition of previously approved project/effort. Significant changes in functionality and/or equipment that require budget actions do not meet the definition of previously approved project/effort.

Expenditures in support of activities not meeting the above criteria are considered to be new projects, not ongoing information technology activities.

Qualification of an information technology activity as a previously approved effort requires an approved FSR AND an approved PIER in accordance with SAM Section 4819.35.

4819.41 PROCUREMENT REVIEW AND CERTIFICATION

(Revised 06/11)

1. Review of Formal IT Solicitations

Formal IT Solicitations as defined in the State Contracting Manual (SCM), Volume 3, Chapter 4, Section B1.0, must be reviewed by the Technology Agency prior to release to the public. Review of Informal IT Solicitations is delegated to departments. The following materials shall be included with the Formal IT Solicitation package:

- a. A completed and signed Formal Information Technology Solicitation Executive Approval Transmittal, which is available in SIMM Section 28A.
- b. All sections, appendices, attachments and exhibits comprising the Formal IT Solicitation.
- c. The Information Technology Procurement Plan prepared in accordance with Volume 3, Chapter 2, Section B3 of the SCM and approved by the DGS.

Review of Formal IT Solicitations is in addition to existing IT-related reporting and approval requirements. The instructions and time frame for submitting Formal IT Solicitations to the Technology Agency for review is specified in SIMM Section 05A.

For addenda focusing on Technical or Functional Requirements within the solicitation that are specific to the California IT Strategic Plan, alignment with the Statewide Enterprise Architecture, or alignment with IT reporting and approval requirements, the Technology Agency will collaborate with the DGS Procurement Division (PD), for DGS-Administered Procurements, and with the issuing department, for delegated procurements, prior to release. All other addenda will only be reviewed by the DGS PD or the issuing department, as appropriate. The time frame for submitting addenda will be determined in collaboration with the Technology Agency and the DGS PD or with the issuing department as appropriate.

Departments shall not be relieved of responsibility for major scope deviations within the Formal IT Solicitations or addenda reviewed by the Technology Agency unless:

- a. The department has specifically informed the Technology Agency-Program Management Office (PMO) in writing of such major deviations at the time of submittal; and
- b. The Technology Agency-OTech has given written approval of the specific deviation.

2. Certification for Information Technology Procurements

A signed certification of compliance with state information technology policies is required for all information technology procurements that cost \$100,000 or more and are in support of a development effort. Development is defined in SAM Section 4819.2 as "Activities or costs associated with the analysis, design, programming, data conversion, acquisition, and implementation of new information technology applications." Procurements of hardware, software, and services (including interagency agreements) are included in this requirement.

A certification is not required for:

- a. Procurements for less than \$100,000;
- b. Procurements limited only to maintenance services;

- c. Procurements in support of previously-approved efforts. See SAM Section 4819.40;
- d. Procurement of services to conduct a feasibility study, provided the services are limited to supporting or conducting the feasibility study and/or preparing the feasibility study report (SAM Sections 4927 and 4928);or
- e. Procurements of excluded activities as described in SAM Section 4819.32.

The certification must be completed by the agency that will directly utilize the procured goods or services, and the original signed certification must be included with the transmittal of the procurement package to the procurement agency or authority. For audit and review purposes, a copy of the signed certification must be retained in the procurement file. The required format for the certification is provided in SAM Section 4832.

3. Certification for Service Contracts

Departments shall complete and sign the Service Contract Information Technology (SCIT) Certification for each proposed service contract and service contract amendment, including non-competitive bids. Please note that IT goods and services, including contracts associated with a Feasibility Study Report (FSR) or FSR Reporting Exemption Request approved by the Technology Agency, would be procured using one of the IT contracting processes developed expressly for IT. In these cases, completion of the SCIT is not necessary, since IT procurements are already subject to Technology Agency review and oversight requirements. The SCIT Certification is available in SIMM Section 16A, and includes instructions for completing and submitting the SCIT Certification.

4819.42 BUDGET CHANGE PROPOSALS

(Revised 03/11)

Budget Change Proposals (BCP) containing specified information technology (IT) components are reviewed by the Technology Agency staff and an evaluation is provided to the Department of Finance Program Budget Manager responsible for review of the agency's budget.

BCPs which request funding for IT projects must be consistent with the agency's Agency Information Management Strategy (see SAM Sections 4900.1-4900.5) and the IT Capital Plan (see SAM Section 4904). The BCP must be supported by an approved Feasibility Study Report (FSR) (SAM Section 4928), or Special Project Report (SPR) (SAM Sections 4945-4945.2) prior to approval of the funding request. In exceptional circumstances, with Technology Agency approval, the funding request may be supported by an approved FSR Reporting Exemption Request or Project Summary Package.

FSRs and SPRs must be submitted in the format and within the time frames specified in SAM, SIMM, and IT Policy Letters issued by the Technology Agency. BCPs must be submitted in the format and within the timeframes specified in annual budget letters issued by Finance. Incomplete or "placeholder" FSRs or SPRs submitted for consideration with an associated BCP may be returned to the agency without consideration.

4832 CERTIFICATION OF COMPLIANCE WITH POLICIES

(Revised 03/11)

The SAM Section 4819.41 specifies that signed certifications of compliance with the state's information technology policies must be included with the transmittal of certain procurement packages to the procurement agency or authority. The required format of the certification is provided in [SAM Section 4832, Illustration 1](#).

Signature Authority Certifications for procurements of \$100,000 or more MUST be signed by the agency director or by a member of agency management specifically designated by the director for this purpose.

As shown in 4832 Illustration 1, the certification must reference one of the following with respect to the justification and approval of the proposed procurement:

1. If the procurement is the result of a Technology Agency-approved Feasibility Study Report (FSR), the project is currently under development, and the Post-Implementation Evaluation Report (PIER) has not yet been approved, provide the project number, the title, and approval date of the FSR. If the procurement is the result of an agency-approved FSR, provide the agency project number, the title, and

approval date of the FSR.

2. If the procurement is an Interagency agreement to procure services from a consolidated data center in support of multiple projects, it must be certified that: (1) the funding level is appropriate for the nature and scope of the services to be supplied; (2) the services are consistent with approved FSRs and/or PIERs; and (3) project reporting for the various projects is current.

Submission of an FSR to the Technology Agency or to the agency director does not constitute project approval. Approval requires an approval letter from the Technology Agency or, for delegated projects, a document indicating approval by the agency director or the director's designee.

4833 INFORMATION TECHNOLOGY ACCESSIBILITY POLICY

(Reviewed 03/11)

It is the policy of the State of California that information and services within California State Government, and provided via electronic and information technology, be accessible to people with disabilities.

State agencies must comply with federal and state laws forbidding discrimination against persons with disabilities, including accessibility of their electronic and information technology. Under existing federal and state laws and policies, state agencies, as well as any contractors working for them, are responsible for ensuring that their agency public Web sites are accessible to both the general public and that their internal agency electronic and information technology systems are accessible by state employees, including persons with disabilities.

California Government Code section 11135 directs that: "state government entities, in developing, procuring, maintaining, or using electronic or information technology, either indirectly or through the use of state funds by other entities, shall comply with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. Sec. 794d), and regulations implementing that act as set forth in Part 1194 of Title 36 of the Code of Federal Regulations."

Government Code section 11135, in requiring compliance with Section 508, mandates that electronic and information technology (EIT) are accessible to individuals with disabilities, specifically:

- State agencies must develop, procure, maintain, or use electronic and information technology, that employees with disabilities have access to and use of information and data that is comparable to the access and use by employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency.
- Individuals with disabilities, who are members of the public seeking information or services from a state agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

4833.1 EXCEPTIONS TO ACCESSIBILITY

(Reviewed 03/11)

The following are exceptions which are allowed for compliance with this policy:

1. A state IT project that is for a "national security system" (FAR 39.204(b) and 36 CFR 1194.3(a)).
2. Acquisition of IT for a state project that is "acquired by a contractor incidental to a contract" (FAR 39.204(c) and 36 CFR 1194.3(b)).
3. A state IT project that is "located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment (FAR 39.204(d) and 36 CFR 1194.3(f))" in what is called the "back-office" exception.
4. Compliance with this policy would present an "undue burden". Undue burden is defined as "a significant difficulty or expense," considering all agency resources available to the program or component for which the product is being procured.

5. No commercial solution is available to meet the requirements for the IT project that provides for accessibility.
6. No solution is available to meet the requirements for the IT project that does not require a fundamental alteration in the nature of the product or its components.

See SIMM Section 25, IT Accessibility Resource Guide, for additional information.

4834 INFORMATION TECHNOLOGY INFRASTRUCTURE POLICY

(Reviewed 03/11)

Agencies Information Technology Infrastructure must enable information sharing across traditional barriers, enhance California's ability to deliver effective and timely services, promote interoperability, support departments and agencies in their efforts to improve government functions, and promote migration to enterprise solutions with reduced complexity and support costs.

4846 CALIFORNIA SOFTWARE MANAGEMENT POLICY

(Reviewed 03/11)

Each agency shall establish and maintain appropriate computer software management practices and ensure that computer software they use and/or have purchased with State funds is legally procured and is used in compliance with licenses, contract terms, and applicable copyright laws. Each agency shall develop and implement policies and procedures to ensure that all staff understand and adhere to proper software management policies.

4846.1 SOFTWARE MANAGEMENT PLAN

(Reviewed 03/11)

To prevent software piracy and promote good software management practices, each agency must maintain a software management program. Each agency must document this effort through a software management plan. See SIMM Section 120 for guidelines on the development and maintenance of this plan.

4846.2 SOFTWARE MANAGEMENT POLICY REPORTING REQUIREMENTS

(Revised 03/11)

Beginning January 31, 2004, and ongoing, each agency shall retain internally for three years, by the agency Chief Information Officer, an annual certification along with the summary of updated inventories conducted by the agency as part of its ongoing software management practices. This certification must also identify the individual responsible for ensuring agency compliance with the California Software Management Policy, SAM Section 4846. In support of this certification, each agency must maintain a detailed inventory report that must be made available upon request to the Technology Agency and/or the Department of General Services. See SIMM Sections 80 and 120 for this and any other reporting requirements.

4851 STATUTORY REFERENCES

(Revised 03/11)

Chapter 834, Statutes of 2006 (SB 834) created the Office of the State Chief Information Officer (OCIO), and its responsibilities were expanded via Chapter 183, Statutes of 2007 (SB 90) as described in Government Code Sections 11545 and 11546.

Chapter 404, Statutes of 2010 (AB 2408), renamed the OCIO the California Technology Agency

(Technology Agency) and transferred the responsibilities of the OCIO to the Technology Agency.

4854 TRAINING AND EMPLOYEE DEVELOPMENT

(Revised 03/11)

General Philosophy. The Technology Agency recognizes that training and employee development are primarily a responsibility of line management. The identification of needs, establishment of priorities, and implementation of training clearly reside with the discretion of each agency. These guidelines relate to technical IT training since management training and development and other general training activities are often intermixed with broader departmental goals. The following statements of policy are intended to facilitate these key objectives.

Policy. Employee training and employee development are the responsibility of each agency. Within an agency, line management is responsible for identification of needed skills, development and implementation of a training plan and establishment of priorities.

Training Coordinator. Agencies should appoint a training coordinator to assist line management in inventorying employee skills, assessing training needs and developing a training schedule. This may be a person in the departmental training office or a person in the IT organization.

Additional responsibilities of the training coordinator will be to act as liaison with other departments for the purpose of joint or coordinated training efforts.

Training Plans. The dynamic field of information technology requires continuous upgrading of skill in order to remain abreast of rapidly changing technology. Because of technological changes and evolving personnel needs, it is imperative that agencies have a plan that will ensure that skills required by the department are developed in an orderly fashion. Management should be aware of the extent to which the effectiveness of their programs are dependent upon the technical skills of their staff.

Training Priorities. It is recommended that priority be given to development of those skills necessary in the effective performance of each person's current position. After essential needs are met, career-related training needs may be addressed.

Source of Training. Agencies should assess their training needs and attempt to satisfy their needs through the most cost-beneficial source. Some training alternatives are: on-the-job training; development of in-house training; cooperative training programs with other departments; training programs through the state data centers; departmental group contracts with outside vendors; and attendance of one or more employees at an outside vendor's training class. The Technology Agency encourages close coordination and cooperation between agencies.

Out-Service Training Needs. Agencies should make every effort to identify those skills areas where they anticipate the need to contract for training with outside vendors. These needs should be outlined in their training plans. Inclusion in the preliminary plans will provide an opportunity to determine whether comparable training may be made available through a more cost-effective source or whether these needs might be coordinated with the needs of other departments.

4900 PURPOSE

(Reviewed 03/11)

Strategic planning is essential to the successful adoption of information technology in state government. An agency information management strategy provides a means of coordinating systems development throughout the agency over the long term. It enables the agency to build systems within a common infrastructure and recognizes that no investment in systems should be made without proper planning. Inherent in the concept of information strategy is the commitment to develop business systems that are based on the real business priorities of the agency.

The purposes of the planning requirements in this section are to ensure that:

1. Agency plans for and uses of information technology are closely aligned with agency business strategies;
 2. Each agency identifies opportunities to improve program operations through strategic uses of information technology; and
 3. Each agency establishes and maintains an information technology infrastructure that supports the accomplishment of agency business strategies, is responsive to agency information requirements, and provides a coherent architecture for agency information systems.
-

4900.1 DEFINITIONS

(Reviewed 03/11)

Agency Information Management Strategy. An agency's information management strategy is the agency's comprehensive plan for using information technology to address its business needs, i.e., to successfully carry out its programmatic mission. Ideally, the agency's information management strategy represents one aspect of a well-defined overall agency business strategy and is therefore closely aligned to its business strategy. If the agency has not established a business strategy, agency staff who are responsible for the agency information management strategy must make assumptions based on their knowledge of the agency's overall mission, its program resources and priorities, and the changing nature of its environment.

Business Strategy. An agency's business strategy is its overall plan for accomplishing its mission in a changing environment with the resources it can reasonably expect to be available. Such a strategy typically addresses the agency's statutory mission and historical role, the expectations of its key stakeholders (individuals and organizations that affect the agency or that the agency affects), the factors that are critical to its success as an organization, the agency's internal strengths and weaknesses, and the political, social, economic, and technological forces in its environment that support or constrain its programs. Business strategies articulate the key issues that must be successfully addressed by the agency and identify the priorities and required resources for proposed actions. A strategy may have a time frame that is as short as a few months, if there is a limited window of opportunity for significant change. However, most agency business strategies present a three- to five-year perspective, with some agencies finding it useful to extend their strategic vision as much as ten to twenty years into the future. Strategic planning is not a one-time effort; it is a fundamental, continuing management process that allows the agency to respond in an effective manner to a changing environment.

Information Technology Infrastructure. An agency's information technology infrastructure is the base or foundation for the delivery of information to support the agency's programs and management. The infrastructure contains elements upon which an agency's information technology activities are dependent. An agency must therefore define, implement, and manage these infrastructure elements to successfully employ information technology.

The desirable characteristics of this infrastructure are efficient support for the exchange of information within the agency and between the agency and other organizations; reliable availability of information processing capabilities whenever and wherever they are needed; preservation of the integrity and confidentiality of information maintained by the agency; sufficient flexibility to allow the timely and efficient addition of new information management capabilities and modifications of established capabilities; and consistency with a coherent set of technical and managerial standards for the employment of information technology.

Typical elements in an information technology infrastructure include:

Application Systems. The applications that an agency purchases and/or develops to achieve personal productivity and program support benefits.

Architecture. The guidelines or blueprints that an agency follows in designing, acquiring, and implementing information technology solutions. Organizationally approved definitions, specifications, and standards are the primary components in an agency's information technology architecture.

Communications. Local area and wide area network components, including linkages with other organizations.

Equipment. An agency's hardware platforms and components ranging from individual personal computers to mainframes and associated peripherals.

Facilities. The electrical, ventilation, fire suppression, physical security, wiring, and other components required

to support an agency's information technology capability, including the physical structure itself.

Funding. Current and projected funding for information technology planning, acquisition, development, and operations activities.

Partnerships. Relationships with other public and private sector organizations that support and enable the agency's pursuit and use of information technology.

People. An agency's technical staff, user community groups, and executive steering and oversight committees that are charged with information technology planning, approval, development, management, operations, and security responsibilities.

Plans. Detailed designs or methods for aligning information technology activities with agency business strategies and accomplishing business objectives. Typical agency information technology plans include strategic, risk management, and operational recovery.

Policies. The rules, conventions, and protocols adopted by the agency to govern the pursuit and use of information technology.

Processes and Procedures. The defined steps for planning, approving, acquiring, developing, operating, maintaining, enhancing, and using information technology within the agency.

Service Definitions. The types of services provided, accepted service levels, and service delivery time frames established for an agency's information technology support organization.

Software. The set of operating system, utility, communications, user interface, and management programs that enable users to operate and control computers and develop application systems.

The infrastructure includes elements owned by the agency and available under contract or through interagency agreement. For agencies that employ the services of a consolidated data center, for example, the required data center resources are considered part of the agency's infrastructure.

Reengineering the Business Process. The search for, and implementation of, radical changes in business processes that result in dramatic efficiencies, reductions in turnaround time, improvements in quality, or improvements in customer service.

Strategic Planning Process for Information Technology. The process of aligning agency plans for, and uses of, information technology with the agency's business strategies.

4900.2 BASIC POLICIES

(Revised 03/11)

Each state agency must establish an ongoing strategic planning process for information technology and submit its strategic plan to the Technology Agency for approval. The strategic planning process established by an agency should be consistent with its needs, resources, uses of information technology, and management style. However, the strategic planning process should:

1. Be consistent with the current statewide strategic direction for information technology, with relevant statewide policies contained in the State Administrative Manual and current management memos, and with agency policies for the management of information and information technology;
2. Include active participation of agency executive and program management;
3. Align agency strategies for information technology with agency business strategies;
4. Identify emerging threats and opportunities in the agency's environment that have a potential impact on the agency's information management and its use of information technology;
5. Assess the strengths and weaknesses of the agency in terms of its information technology infrastructure and information management capabilities;
6. Assess the potential of new information technologies to enable new business strategies and further the accomplishment of established strategies;

7. Provide for the creation and maintenance of an agency information technology infrastructure that will support agency information requirements and business strategies; and
8. Establish goals and priorities for the acquisition of new information management capabilities.

Each agency may determine the format and content of the documentation of its strategic plan for information technology. The documentation must satisfy agency management requirements and be sufficiently detailed to provide the Technology Agency with a clear understanding of the agency's information management strategy. Agency Information Management Strategy (AIMS) documentation guidelines can be found in SIMM Section 110.

It is the responsibility of the agency to ensure that the information available to the Technology Agency represents its current strategy. The Technology Agency will base its decisions regarding the approval of an agency's information technology activities and support for its budget augmentations in part upon its understanding of the Agency's Information Management Strategy (AIMS) and the relationship between the AIMS and the agency's overall business strategy. In general, activities and proposals that are not supported by an AIMS that meets the basic requirements of this section or that are inconsistent with an agency's established strategy will not be approved or supported by the Technology Agency. Any agency that does not have an approved AIMS will have all information technology project delegation rescinded, including delegation for expenditures under the Desktop and Mobile Computing Policy (SAM Section 4989.)

The agency must submit documentation of its information management strategy to the Technology Agency at the time it completes its initial strategic planning effort and, thereafter, whenever there is a significant change in strategy. SAM Section 4900.3 provides guidelines for the AIMS documentation that must be submitted to the Technology Agency. Additionally, the agency must annually certify that the AIMS approved by the Technology Agency represents its current strategy. See SAM Section 4900.5 and SIMM Section 60.

Note that approval of an agency's AIMS does not imply approval of specific projects, nor does it guarantee funding for the plan or specific projects an agency may initiate under the plan. Project funding must be addressed through the budget process, where final determination will be based on statewide as well as agency priorities.

4900.3 AGENCY INFORMATION MANAGEMENT STRATEGY DOCUMENTATION

(Revised 03/11)

Each agency is expected to tailor the documentation of its information management strategy to its own needs and to provide the Technology Agency with sufficient information for the Technology Agency to understand that strategy in light of the agency's overall business strategy. AIMS documentation guidelines can be found in SIMM Sections 60 and 110.

Agencies are requested to address at least the following in their submittal to the Technology Agency:

Changes in Mission and Programs. A summary of expected changes in the agency's mission and programs that will require changes to the agency's information management capabilities.

Agency Business Strategy. A summary of the agency's business strategy for the period covered by the information management strategy.

Information Technology Vision. A summary of the agency's values and principles that articulate the conceptual basis or foundation for the agency's chosen information technology infrastructure.

Impact on Information Management. An assessment of the impact of the agency's business strategy upon its information management practices.

New Information Technologies. A statement of how new information technologies will be employed in the business strategy.

Current Information Technology Infrastructure. A description of key elements in the agency's current information technology infrastructure: standards, hardware, software, communications, personnel, partnerships, and application systems.

Planned Information Technology Infrastructure. A description of how that infrastructure will be developed or leveraged to meet future information requirements.

Information Management Priorities, Objectives, and Resources. A statement of the agency's priorities, objectives, and resources for achieving the development or acquisition of new information management capabilities.

Activities to Reengineer Agency Business Processes. A description of changes the agency has made, or is making, to restructure its business operations in an effort to achieve dramatic improvements in critical measures of performance, such as efficiency, turnaround time, customer satisfaction, and quality.

An agency may prepare a separate summary of its information management strategy for submission to the Technology Agency or it may choose to provide the Technology Agency with copies of its internal documents. The Technology Agency may request additional information to clarify its understanding of an agency's strategy. Agencies are encouraged to submit informational copies of their business strategies with their information management strategies and to provide oral briefings to the Technology Agency in conjunction with submitting their strategies.

4900.5 AGENCY INFORMATION MANAGEMENT STRATEGY REPORTING REQUIREMENTS (Revised 03/11)

The AIMS must be submitted to the Technology Agency at the time the agency completes its initial strategic planning effort. A revised AIMS must be submitted to the Technology Agency for approval whenever there is a significant change in the agency's strategy. Additionally, to assist the Technology Agency in reviewing an agency's information technology BCPs (see SAM Section 4819.42), the agency annually must certify, by August of each year, or as instructed by the Technology Agency, that the AIMS approved by the Technology Agency represents its current strategy. SIMM Section 60 provides a template for the AIMS transmittal letter, which must be signed by the agency director or chief deputy director, for this annual certification.

4903 EXHIBITS AND SUPPORTING DOCUMENTS (Reviewed 03/11)

The documents required in SAM Sections 4903.1-4903.4 supplement the information in the agency's AIMS by providing details about the organization or information management within the agency and the resources available to the agency.

4903.1 INFORMATION MANAGEMENT ORGANIZATION (Revised 03/11)

By June 30 of each year, or as instructed by the Technology Agency, each agency must submit to the Technology Agency organization charts showing:

1. The relationship between the organizational unit or units responsible for information management functions (including telecommunications) and other units within the agency; and
2. The internal organization of the unit or units responsible for information management functions, including telecommunications. The internal organization chart should indicate numbers of positions by classification.

4903.2 INFORMATION MANAGEMENT COSTS (Revised 03/12)

By February 1 of each year, or on an annual basis, as instructed by the Technology Agency, each agency is required to summarize its actual and projected information technology costs for the past year, and current year. The format and instructions for submittal required by the Technology Agency are specified in Section 55 of the SIMM.

4904 INFORMATION TECHNOLOGY FIVE-YEAR CAPITAL PLAN

(Revised 03/11)

To forge the necessary integration of the business and IT functions in California state government, state Agencies are required to prepare and submit a Five Year IT Capital Plan (Agency IT Capital Plan) for review by the Technology Agency and the Department of Finance. These plans will serve to inform the Statewide Five Year IT Capital Plan. The Agency IT Capital Plans will:

- Ensure that IT investments drive program efficiency and effectiveness and improve the quality of government services for Californians.
- Facilitate improvements in internal business processes and financial management through IT investments.
- Link IT investments to state and agency priorities and business direction.
- Promote the alignment of IT investments with the Agency's enterprise architecture (Technology, Standards, and Infrastructure).
- Enhance and promote enterprise data sharing through IT investments.
- Facilitate consideration and conceptual approval to pursue selected IT investments.

The scope of the Agency IT Capital Plans will include (see SIMM Section 57):

- All projects or IT investments (including infrastructure changes) that are proposed for initiation during a five year period; and
- The documentation necessary for the Technology Agency to provide conceptual approval.

The Agency IT Capital Plans must be updated annually or more frequently as needed and do not eliminate the requirement for a detailed business case for conceptually approved IT projects.

The Statewide IT Capital Plan will represent the Administration's plan for strategic IT investments and will be supported by the Governor's Budget, the CIO's Statewide IT Strategic Plan, Budget Change Proposals, and Feasibility Study Reports.

4906 - ENTERPRISE ARCHITECTURE

(Revised 03/11)

The statewide Enterprise Architecture (EA) is developed in a cooperative, managed, and coordinated effort facilitated by the California Technology Agency. The National Association of State Chief Information Officers methodology and the Federal Enterprise Architecture framework included in SIMM Section 58A are adopted as the state's standards to develop and maintain the statewide EA.

Accordingly, state agencies shall implement EA in accordance with SIMM Section 58D. In addition, state agencies shall, to the extent practical, utilize the EA Practices included in SIMM Section 158.

4910 - CALIFORNIA PROJECT MANAGEMENT METHODOLOGY (CA-PMM)

(Reviewed 03/11)

The California Project Management Methodology (CA-PMM) is based on project management best practices

as described in the project Management Institutes Project Management Body of Knowledge (PMBOK). The purpose of the CA-PMM is to provide consistent project information regardless of the state agency that is managing the project to provide policymakers greater visibility as to the status of IT projects and enable project executives, control agencies, and other interested parties to review and evaluate the status of IT projects as well as provide informed direction and guidance to IT Project Managers.

The CA-PMM provides the framework for the entire Project Management Cycle from project concept to maintenance and operations. Included in the CA-PMM are a set of templates to support the Project Management Life Cycle and a Reference Manual that contextualizes the different elements of the Project Management Life Cycle. See SIMM Section 17 for the Toolkits, the Reference Manual, and the specific conditions for utilizing the CA-PMM.

4920 PURPOSE

(Reviewed 03/11)

The feasibility study represents the first opportunity for agency management to assess the full implications of a proposed information technology project. The feasibility study is also the means of linking a specific information technology project to the agency's strategic business plans and information technology plans, and to ensure that the proposed project makes the best use of the agency's information technology infrastructure. The purposes of the feasibility study are to:

1. Determine whether there is a business case for a proposed project, i.e., whether the expenditure of public resources on the project is justified in terms of the project's:
 - a. Being responsive to a clearly-defined, program-related problem or opportunity;
 - b. Being the best of the possible alternatives;
 - c. Being within the technical and managerial capabilities of the agency; and
 - d. Having benefits over the life of the application that exceed development and operations costs. Project benefits typically include reduced program costs, avoidance of future program cost increases, increased program revenues, or provision of program services that can be provided only through the use of information technology.
 2. Provide a means for achieving agreement between agency executive management, program management, and project management as to:
 - a. The nature, benefits, schedule, and costs of a proposed project; and
 - b. Their respective management responsibilities over the course of the project.
 3. Provide executive branch control agencies and the Legislature with sufficient information to assess the merits of the proposed project and determine the nature and extent of project oversight requirements.
-

4921 FEASIBILITY STUDY BASIC POLICY

(Reviewed 03/11)

A feasibility study must be conducted prior to the encumbrance or expenditure of funds on any information technology project. For most projects, the feasibility study must be conducted in conformance with SAM Sections 4922 through 4927. The only exception to this requirement is the acquisition of desktop and mobile computing commodities under the Desktop and Mobile Computing Policy. (See SAM Section 4989.) In addition, a Feasibility Study Report (FSR), which documents the feasibility study, must be approved prior to the encumbrance or expenditure of funds, including the use of staff resources, on any information technology project beyond the feasibility study stage. For most projects, the FSR must be prepared in accordance with SAM Section 4928. For projects that have been delegated to the agency director and whose costs fall below a specified level, the feasibility study may be documented by means of a Project Summary Package. See SAM Section 4930 and SIMM Section 20.

The FSR must be reviewed and approved in accordance with the general requirements of SAM Sections 4819.3-4819.42 (State Information Management Authority and Responsibility), as well as the specific requirements of Sections 4926-4930.1. See SIMM Section 20 for FSR Preparation Instructions.

4922 FEASIBILITY STUDY SCOPE

(Reviewed 03/11)

The scope of the feasibility study must be commensurate with the nature, complexity, risk, and expected cost of the proposed use of information technology.

The study must provide sufficient information to assure agency program management that the proposed response meets program requirements. The study also must provide sufficient information to allow agency executive management to make a sound decision as to the merits of the proposed response as an investment of public resources.

4923 FEASIBILITY STUDY PARTICIPATION

(Reviewed 03/11)

The feasibility study must be based on an understanding of the needs, priorities, and capabilities of: (1) the users of the information that is to be provided; and (2) the agency unit or program that will have operational responsibility for the information technology application. Representatives of program management and staff must participate in the feasibility study process.

4924 FEASIBILITY STUDY DOCUMENTATION

(Revised 03/11)

The SAM Section 4928 and instructions and guidelines published by the Technology Agency (see SIMM Section 20) specify the content of the FSR, which must provide a complete summary of the results of the feasibility study. In addition to the FSR, the agency must maintain sufficient documentation of each study to ensure that project participants, agency management, and control agency personnel can resolve any questions that arise with respect to the intent, justification, nature, and scope of the project.

4925 CONSISTENCY WITH AGENCY INFORMATION MANAGEMENT STRATEGY AND IT CAPITAL PLAN

(Reviewed 03/11)

Each proposed project must be consistent with the agency's overall strategy for the use of information technology, as expressed in its current Agency Information Management Strategy (see SAM Sections 4900.2-4900.6) and IT Five-Year Capital Plan (see SAM Section 4904).

4927 FEASIBILITY STUDY PROCESS

(Reviewed 03/11)

Each agency must follow a systematic, analytical process for evaluating and documenting the feasibility of information technology projects, as defined in SAM Section 4819.2. This process must include:

1. Developing an understanding of a problem (or opportunity) in terms of its effect on the agency's mission and programs;
 2. Developing an understanding of the organizational, managerial, and technical environment within which a response to the problem or opportunity will be implemented;
 3. Establishing programmatic and administrative objectives against which possible responses will be evaluated;
 4. Preparing concise functional requirements of an acceptable response;
 5. Identifying and evaluating possible alternative responses with respect to the established objectives;
 6. Preparing an economic analysis for each alternative that meets the established objectives and functional requirements;
 7. Selecting the alternative that is the best response to the problem or opportunity;
 8. Preparing a management plan for implementation of the proposed response; and
 9. Documenting the results of the study in the form of a Feasibility Study Report (FSR), as specified in SAM Section 4928.
-

4928 FEASIBILITY STUDY REPORT

(Revised 03/11)

The FSR must provide an accurate summary of the results of the feasibility study. As with the study itself, the scope of the FSR must be commensurate with the scope and complexity of the problem or opportunity being addressed. Enough technical detail must be included in the FSR to show that the proposed response to the problem or opportunity is workable and realistic. The FSR must provide a basis for understanding and agreement among project management, executive management and program management, as well as satisfy the information requirements of state-level control agencies.

The FSR must be submitted to the Technology Agency and to the Office of the Legislative Analyst. In addition, the FSR must be submitted to the Department of General Services when the contract total exceeds the agency's delegated purchasing authority threshold. FSRs must be submitted in a format specified by the Technology Agency and signed by the agency director or his/her designee. The Technology Agency publishes detailed instructions and guidelines for agencies' use in preparing FSRs. A copy of the instructions, guidelines, and required forms is available in SIMM Section 20. The instructions and guidelines specify the MINIMUM amount of information necessary for the Technology Agency's approval of the FSR.

The FSR must provide a complete summary of the results of the feasibility study and establish the business case for investment of state resources in a project by setting out the reasons for undertaking the project and analyzing its costs and benefits. Documentation provided by the agency must contain at least the following information:

1. A description of the business problem or opportunity the project is intended to address.
2. The project objectives, i.e., the significant results that must be achieved for an alternative to be an effective response to the problem or opportunity being addressed.
3. A thorough description of the selected alternative, including the hardware, software and personnel that will be used.
4. A discussion and economic analysis of each of the alternatives considered in the feasibility study that meets the established objectives and functional requirements, and the reasons for rejecting the alternatives that were not selected.
5. A complete description of the information technology capabilities and the conditions that must exist in order to satisfy each defined objective.
6. An economic analysis of the life cycle costs and benefits of the project and the costs and benefits of the

current method of operation during the life cycle of the project.

7. The source of funding for the project.
8. A detailed project schedule showing key milestones during the project's life.

A Project Summary Package (SAM Section 4930) must be prepared and included in the FSR.

The agency must maintain sufficient documentation of each study to ensure that project participants, agency management, and control agency personnel can resolve any questions about the intent, justification, nature, and scope of the project.

4930 PROJECT SUMMARY PACKAGE

(Reviewed 03/11)

A Project Summary Package must be prepared and included in each FSR and SPR. In addition, the Project Summary Package may be used to document the feasibility study for projects with a total development cost equal to or less than ten percent of the agency's cost delegation threshold. See SAM Section 4819.39.

See SIMM Section 20 and/or 30 for instructions for completing the Project Summary Package.

4940 PROJECT OVERSIGHT AND PROJECT IMPLEMENTATION AND EVALUATION POLICY

(Revised 03/11)

Agencies must establish project reporting and evaluation procedures for each approved information technology project. The scope of these procedures must be commensurate with the overall scope of the project's associated risk to the state.

The fundamental requirements for project oversight and evaluation are specified in SAM Sections 4819.30-39 - 4819.42. All projects, including projects delegated by the Technology Agency to the agency director, are subject to those requirements. Projects that have been delegated to the agency director in accordance with SAM Section 4819.36 require appropriate project reporting by the project manager to the agency director.

4941 OVERVIEW

(Revised 03/11)

Once the FSR for an information technology project has been approved the project may proceed, contingent upon any conditions imposed by the Technology Agency. Throughout the project phases, agency management must follow the IT Project Oversight Framework (see SIMM Section 45) to provide the appropriate level of independent project oversight, project management practices and project risk assessments to ensure the success of the project.

Post-Implementation and Evaluation Report. Following completion of each information technology project, a post-implementation evaluation must be carried out by the agency. The evaluation should:

1. Measure the benefits and costs of a newly-implemented information technology application or system against the most recently approved project objectives; and
 2. Document projected operations and maintenance costs over the life of the application or system.
-

4942 COMPLIANCE REVIEW

(Revised 03/11)

Specific projects or agencies as a whole may be subject to compliance reviews conducted by the Technology

Agency. The purposes of a compliance review are to verify agency adherence to statewide information technology policies as well as approved agency policies, and to determine agency fulfillment of approved plans. The Technology Agency will review project reporting documentation in conjunction with its compliance review and oversight responsibilities.

The Technology Agency may impose sanctions, such as a reduction or elimination of an agency's delegated cost threshold for reporting and approval of IT projects by the Technology Agency, or other sanction deemed appropriate by the Technology Agency, upon finding that a state agency is consistently and/or willfully out of compliance with state policies.

4943 AUDIT OF INFORMATION TECHNOLOGY PROJECTS

(Revised 03/11)

All information technology projects are subject to audit, with project reporting and evaluation documents an essential aspect of the audit trail. Documentation supporting project decisions must be kept by the agency for a minimum of two years following approval of the post-implementation assessment.

Some projects may be subject to ongoing review by the Office of State Audits and Evaluations (OSAE). OSAE may review the Feasibility Study Reports of projects approved by the Technology Agency and the Feasibility Study Report - Reporting Exemption Requests of projects delegated to agencies by the Technology Agency. OSAE will select projects for ongoing review based on their risk, cost, and materiality.

For projects selected for ongoing review, OSAE will develop and submit to agency management periodic status reports and the project Post-Implementation Evaluation Report (PIER) required under SAM Section 4947. Agencies are required to submit final versions of the periodic status reports and the project PIER to the Technology Agency within five working days after they are received from OSAE.

If OSAE determines that the project should be audited, the agency must enter into an interagency agreement with OSAE for that purpose. Since the cost that the agency otherwise would have incurred in monitoring the project and producing progress reports and the PIER will no longer be borne by the agency, these costs should not be included in the project budget. However, the agency should ensure that the project budget includes an amount sufficient to cover the costs of the interagency agreement with OSAE.

4944 IT PROJECT OVERSIGHT AND REPORTING

(Revised 03/11)

The Technology Agency will conduct Agency, department, IT project management and oversight assessments designed to provide agency management and the Technology Agency information on the progress of a project, including compliance with the minimum requirements for IT project management, project risk management, project oversight and project reporting activities at the agency and control agency levels as outlined in the IT Project Oversight Framework (see SIMM Section 45). The Technology Agency will schedule assessment based on an established criteria.

Independent Project Oversight Reports (IPORS) are required to be submitted on a regular basis based on project criticality to the Technology Agency (see SIMM Section 45).

4945 SPECIAL PROJECT REPORT—GENERAL REPORTING REQUIREMENTS

(Revised 03/11)

Preparation of an SPR is required whenever a project substantially deviates from the costs, benefits or

schedules documented in the approved FSR, when a major revision occurs in project requirements or methodology, when criteria listed in SAM Section 4819.37, other than the project's cost exceeding the level the Technology Agency may have delegated to the agency, arise during the development or implementation of the project, or when a significant change in state policy draws into question the assumptions underlying the project. No encumbrance or expenditure of funds shall be made to implement an alternative course of action until approval has been received from the Technology Agency or the agency director, as appropriate. SAM Section 4819.36 lists specific conditions that require submission of an SPR to the Technology Agency.

If an SPR for a delegated project must be submitted to the Technology Agency, the agency must attach to the SPR a copy of the approved Feasibility Study Report and the Transmittal signed by the agency director or his/her designee.

The SPRs which must be submitted to the Technology Agency should be transmitted within 30 days after recognition of a substantial deviation. The SPR must be submitted to the Technology Agency and the Office of the Legislative Analyst. SPRs must be submitted in a format specified by the Technology Agency and signed by the agency director or the director's designee. See SIMM Section 30 for SPR Preparation Instructions.

4945.2 SPECIAL PROJECT REPORT—CONTENT AND FORMAT

(Revised 03/11)

The SPR must provide sufficient information for agency management, executive branch control agencies, and the Legislature to assess the merits of the proposed project change and determine the nature and extent of future project oversight requirements. If a SPR lacks sufficient information for these purposes, the Technology Agency will request that the agency provide additional information.

Information provided in the SPR must be commensurate with the level of deviation of costs, benefits, timelines, or project requirements from those of the approved FSR or last approved SPR.

The SPRs must be submitted in a format specified by the Technology Agency and signed by the agency director or his/her designee. The MINIMUM content for an SPR is project status, an explanation of the reason for the project deviation, a revised project management schedule, and economic summary information. The Technology Agency publishes instructions and guidelines for agencies' use in preparing SPRs. See SIMM Section 30 for SPR Preparation Instructions.

4946 MAINTENANCE AND OPERATIONS PLAN POLICY

(Revised 03/11)

The Maintenance and Operations (M&O) Plan provides an orderly, cost effective and planned process for ongoing routine M&O activities of implemented information technology (IT) systems.

The Technology Agency may request agencies to submit an M&O Plan for IT projects. Agencies requested to submit an M&O Plan must have the plan approved by the Technology Agency before commencing M&O activities. Once an M&O Plan is approved, agencies must provide the Technology Agency annual updates. The Technology Agency can suspend or withdraw its approval of the M&O Plan to respond to changing circumstances.

See the Statewide Information Management Manual M&O Plan Guidelines located in SIMM Section 160.

4947 POST-IMPLEMENTATION EVALUATION REPORT

(Revised 03/11)

Unless the agency has entered into an interagency agreement with the Office of State Audits and Evaluations (OSAE) under SAM Section 4943, a post-implementation assessment must be carried out by the agency

following the completion of each information technology project. No project is considered complete until the report of that assessment, the Post-Implementation Evaluation Report (PIER), has been approved by the Technology Agency or by the agency director, as appropriate. Approval of a PIER by the Technology Agency or the agency director, as appropriate, terminates the project reporting requirements.

If OSAE selects the project for review under SAM Section 4943, OSAE will conduct the post-implementation assessment and submit the PIER to agency management. The agency is required to submit the PIER to the Technology Agency within five working days after it is received from OSAE.

The post-implementation assessment must be conducted after the new information technology capability has been operational for a sufficient period of time for its benefits and costs to be accurately assessed. Initial operational problems must have been resolved and sufficient experience and data must have been accumulated to determine whether the project met the proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits. The optimum time after implementation to conduct the assessment depends upon the nature of the project. Six months to one year after implementation is typical. The assessment MUST be completed within 18 months of project completion. Agencies are required to follow the instructions for preparing and submitting the PIER and Transmittal Letters, see SIMM Section 50.

4947.2 POST-IMPLEMENTATION EVALUATION REPORT—CONTENT AND FORMAT

(Revised 03/11)

The PIERs must be submitted in a format specified by the Technology Agency and signed by the agency director or his/her designee, see SIMM Section 50. The level of detail included in the Post-Implementation Evaluation Report must be commensurate with the scope and complexity of the project and its anticipated benefits. The narrative portion of the PIER for a minor project can be as brief as one or two pages. However, it must provide sufficient information for agency management, executive branch control agencies, and the Legislature to assess the success of the project. In particular, the PIER must contain a comparison of the timelines, costs and benefits forecast by the FSR with the actual timelines, costs and benefits of the project. If the project was a limited success or involved significant differences between expectations and results, the agency must present the actions it intends to take to improve the outcome. If the project was a failure and the problem or opportunity that led to the project still exists, the agency must present the actions it intends to take to address that problem or opportunity.

4981 INTRODUCTION

(Reviewed 03/11)

No single combination of information technology and management philosophy can be identified as being universally suitable for state government, nor can pre-determined rules be established to allow the routine assignment of a new application to the particular combination of technology and management practice which will be most appropriate. Each decision regarding a choice of information technology and management structure must be made on a case-by-case basis, considering the particular circumstances of the application and the particular technological and managerial options available.

4981.1 POLICY

(Reviewed 03/11)

The decision to select a particular technological approach must take into account the full range of significant factors which will influence the success of the application during its operational life. These significant factors include:

1. **Statutes, Regulations and Policies**-This factor consists of applicable statutes, regulations and policies which could impact a decision to use information technology.
 2. **Agency Management**-This factor includes assessment of the agency's prior experience with information technology and the managerial resources it can bring to bear on the use and control of the technology, i.e., whether the agency has an appropriate management infrastructure and agency personnel possess the necessary qualifications.
 3. **Cost**-Applications of information technology must be reviewed in terms of their cost justification. Such review must take into account the potential impact of the application on the overall economy of state operations. Assessment of the costs associated with each technological alternative must cover a sufficient time span to allow for reasonable amortization of start-up costs as well as realization of cost savings and cost avoidance potentials.
 4. **Nature of the Application**-This factor encompasses (1) the extent to which the application is critical to the accomplishment of the agency's mission, goals and objectives, (2) the degree of centralization or decentralization required for this activity, (3) the data communication requirements associated with the activity, (4) the characteristics of the data to be collected and processed, i.e., source, volume, volatility, distribution, and security or confidentiality, (5) the urgency of the application, and (6) backup requirements for personnel, software, data and hardware.
 5. **Hardware Considerations**-This factor includes review of the alternative hardware configuration options capable of effecting the successful implementation of a given information technology activity. Consideration must be given to (1) compatibility with existing hardware, including telecommunications equipment, (2) physical plant requirements necessary for proper operation of the equipment, (3) hardware maintenance, (4) the knowledges and skills required of state personnel, (5) backup processing capability, and (6) the existing capacity, immediate required capacity and future capacity.
 6. **Software Considerations**-This factor includes a review of the software options available to achieve successful implementation of a given information technology activity. Consideration must be given to (1) the compatibility of computer languages with existing and planned activities, (2) maintenance of the proposed software, e.g. vendor-supplied, (3) the urgency of the application, (4) the knowledges and skills required of state personnel, (5) the availability of complete documentation, and (6) the availability of necessary security features.
 7. **Interagency Considerations**-This factor includes analyzing the agency's interfaces with other state agencies, or federal or local government. Consideration must be given to compatibility of communications and sharing of data.
-

4982 INTRODUCTION

(Revised 09/08)

Government Code Chapter 5.5 and 7.5 define two consolidated data centers in state government: 1) the Hawkins Data Center in the Department of Justice, and 2) the Department of Technology Services (DTS) in the State and Consumer Services Agency. Other data processing centers are considered single-agency, dedicated-use data processing centers rather than consolidated data processing centers. All data centers shall adhere to the following center policies.

4982.1 DATA CENTER CONSOLIDATION AND DETERMINATION OF AGENCY-DATA CENTER ASSIGNMENTS

(Revised 03/11)

It is the state's policy to transition out of non-Tier III data centers and server rooms and to end upgrades during the transition, unless there is an emergency. The following policy shall be used to determine an agency's Tier III-equivalent facility assignment for services, and to ensure consolidation activities proceed timely:

1. The Hawkins Data Center shall serve as the Tier III-equivalent for the Department of Justice.

Agencies assigned to other state-designated Tier III-equivalent facilities whose official business requires access to the data contained in the California Criminal Justice Information System's (CJIS) data repositories, including those agencies utilizing the California Law Enforcement Telecommunications System (CLETS), shall access CJIS serviced data repositories and CLETS through the Hawkins Data Center.

2. The Department of Water Resources Data Center serves as the Tier III-equivalent facility for the Natural Resources Agency and its associated departments.
 3. The Franchise Tax Board (FTB) Data Center serves as the Tier III-equivalent data center for the FTB.
 4. The following Office of Technology Services (OTech) facilities shall serve as the Tier III-equivalent Data Centers for all other agencies in the state:
 - a. The OTech Gold Camp Data Center serves as the production data center for the Executive Branch. In addition, the Gold Camp Data Center manages services and provides disaster recovery services to all state agencies not identified in 1, 2, and 3 above.
 - b. The Federal Data Center (FDC) located at the OTech Gold Camp facility serves as a physically partitioned-off Data Center shared by agencies.
 - c. The OTech Vacaville Data Center serves as a disaster recovery site with a secondary role as a production data center.
 - d. Any other Tier III-equivalent facility designated by the Technology Agency.
 5. To facilitate timely completion of consolidation activities:
 - a. The OTech Customer Owned Equipment Managed Services (COEMS) is discontinued. COEMS customers will transition to one of the state's Tier III-equivalent facilities previously referenced.
 - b. Department server rooms will be closed.
 - c. File and print services in the greater Sacramento area will be consolidated.
 - d. New applications, server refreshes, storage replacements, and new virtualization clusters shall be located at a state Tier III-equivalent facility.
 - e. Agencies shall review all IT projects that are in progress in order to plan transition of servers and storage to a state Tier III-equivalent facility.
 - f. The Computer Room Construction policy and requirements established in ITPL 09-04 remain in effect.
 - g. Facility upgrades for server rooms designated for shutdown will be limited to emergencies. Agencies shall utilize the approval procedures described in ITPL 09-04.
 6. Agencies shall use the Data Center Consolidation Survey and Assessment (S&A) included in SIMM Section 67, and will be reporting to the Technology Agency PMO in accordance with the timeframes and submittal instructions included in SIMM Section 05A.
-

4982.2 POLICIES FOR DATA CENTER MANAGEMENT

(Revised 03/11)

Data Center Mission—Each data center shall have a statement of mission which states the data center's objectives and outlines the services provided by the center.

Data Center User Interaction—

1. Each data center shall have a functional responsibility to provide liaison with the users of the center. This shall include establishing and maintaining user groups and forums appropriate to the requirements of the users and the mission of the center.
2. Each data center shall make readily available a data center user guide which shall contain

detailed and up-to-date descriptions of and instructions for the use of the various services offered by the center. This guide should describe the operational management processes required by user agencies to avail themselves of data center services including resources scheduling, problem management, system backup and recovery procedures and data communications network management.

Data Center Financial Management—See SAM Section 6780 for the financial management policy applicable to the Office of Technology Services.

Exchange of Data Between Data Centers—The exchange or transfer of data between data centers by intercoupling or telecommunications shall be made only with the approval of the Technology Agency. Requests for approval to exchange or transfer data between data centers must contain programmatic justification and describe how the exchange or transfer will be accomplished. The request must also clearly describe what safeguards will be established to provide data confidentiality and security in compliance with SAM Sections 5300-5399, Security and Risk Management Policy.

This section does not prohibit the transmission of data from the Department of Motor Vehicles to the Hawkins Data Center in order to obtain vehicle registration and driver license data for criminal justice purposes, or the transmission of data between centers in the same state agency.

4989 DESKTOP AND MOBILE COMPUTING POLICY

(Revised 12/08)

In lieu of a Feasibility Study Report submitted to the Technology Agency, the Technology Agency delegates authority to acquire desktop and mobile computer commodities to agencies that have submitted acceptable Disaster Recovery Plans (DRP) or DRP certifications, maintain compliance with all applicable state IT security provisions as defined in SAM Sections 5300-5399, and have appropriate plans for the use of desktop and mobile computing commodities.

Under the Desktop and Mobile Computing Policy, agencies may acquire desktop and mobile computing commodities necessary to support the agency's programmatic functions and business needs. This includes acquiring desktop and mobile computing commodities to support increased staffing, as well as the ongoing replacement of obsolete or nonfunctioning desktop and mobile computing commodities. Desktop and mobile computing configurations are expected to make use of proven, "off-the-shelf" hardware and software. Specific exclusions from this policy are listed in Section 4989.2 below.

Replacement of desktop and mobile computing commodities acquired as part of a previously approved IT project, as defined in SAM Section 4819.2, may be included in this policy as much as such commodities are incorporated into and are no longer distinguishable from the agency's IT infrastructure.

4989.1 - DEFINITION OF DESKTOP AND MOBILE COMPUTING

(Revised 03/11)

Communication - For the purpose of interpreting this policy, communication is the requesting, sending, transmitting, or receiving of electronic data via cable, telephone wire, wireless, or other communication facility.

Desktop and Mobile Computer Software - Commercially licensed software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Computer Supplies - Consumable commodities used for data storage, printing, and/or other IT supplies as defined in SAM Section 4919.2.

Desktop and Mobile Computing - For the purposes of this policy, desktop and mobile computing is the use of desktop and mobile computing commodities in support of state agencies' business operations.

Desktop and Mobile Computing Commodities - Hardware and software commonly required for most state employees to perform daily business transactions such as desktop computers, mobile computers, (e.g., personal digital assistants, laptop computers, smartphones), desktop and mobile computer software, servers,

server software, peripheral devices (e.g., printers), supplies, and LAN infrastructure.

Desktop and Mobile Computing Servers - Computer servers necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop and Mobile Server Software - Commercially licensed server software necessary for the operation, use, and/or security of desktop and mobile computers.

Desktop Computers - Computing devices, generally designed to remain in a fixed location, that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an agency's IT infrastructure and/or data systems.

Information Technology Asset Management - The effective tracking and managing of IT assets for an agency's program and enterprise IT infrastructure and production systems, including the ability to identify and classify agency-owned hardware and software, telecommunications, maintenance costs and expenditures, support requirements (e.g., state staff, vendor support), and the ongoing refresh activities necessary to maintain the agency's IT assets.

Information Technology Infrastructure – An agency's platform for the delivery of information to support agency programs and management. Included in the infrastructure are equipment, software, communications, rules, and vision.

Local Area Network (LAN) – Two or more desktop or mobile computers at the same site connected by cable, telephone wire, wireless or other communication facility providing the ability to communicate or to access shared data storage, printers, or other desktop and mobile computing commodities.

Mobile Computers - Portable-computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to an agency's IT infrastructure and/or data systems.

Remote Access - The connection of an information asset from an off-site location to an information asset on state IT infrastructure.

Smartphone - A mobile computing device that provides advanced computing capability and connectivity, and runs a complete operating system and platform for application developers and users to install and run more advanced applications.

Wide Area Network (WAN) - Two or more physical locations connected by cable, wire, or other wireless transmission, providing the ability to communicate between locations and/or Internet connectivity.

4989.2 - EXCLUSIONS

(Revised 03/11)

The following activities are excluded from the Desktop and Mobile Computing Policy and must be treated in accordance with SAM Sections 4819.3 through 4819.42.

IT Projects - As defined in SAM Section 4819.2, beyond the acquisition, installation, and operation of DMCP commodities as defined in this policy. The acquisition of desktop and mobile computing commodities required for an IT project, whether reportable or delegated, must be included within the project scope and acquired under the approved project's authority. Use of this policy to circumvent IT project reporting requirements or to make an otherwise reportable project fall within delegated thresholds is expressly prohibited.

Budget Actions - Any acquisition, maintenance, or support of desktop and mobile computing commodities which requires a Budget Change Proposal, a Budget Revision, or other budget action is not covered by the Desktop and Mobile Computing Policy. However, this policy may be used to acquire the standard complement of desktop and mobile computing commodities as approved by the Department of Finance for new positions.

Specialized or Single-Purpose Systems - Acquiring any specialized, single-purpose, non-modifiable system, such as computer-aided design systems, desktop publishing systems, programmer workbench systems, or artificial intelligence systems is excluded from this policy. However, software-based applications used on a general-purpose personal computer may be covered by the policy. For example, desktop publishing employing word processing, graphics, and page layout software packages on a general-purpose personal

computer falls within this policy; desktop publishing employing a specialized computer system that has been developed and marketed for the sole purpose of doing desktop publishing does not. A specialized, single-purpose system that allows some connectivity to an agency's existing systems, such as electronic mail, is still considered a specialized or single-purpose system for the purposes of this policy.

Infrastructure or Platform Migration - Acquisitions associated with or mandated by a change in an agency's standard technical architecture for servers, desktops and/or mobile computing platforms are excluded from the policy. Migrating to a newer version within the existing standard's product family is not considered an infrastructure or platform migration.

Wide Area Networks (WAN) - The acquisition, maintenance, or support of desktop and mobile computing commodities specifically to install or operate a WAN are excluded from the policy. These activities for WANs are considered IT projects, or components of IT projects, for the purposes of this policy. However, upgrading the capacity of a previously approved WAN project may fall within the definition of a previously approved project. (See SAM Section 4819.2: "Previously Approved Effort/Project".)

While the acquisition of desktop and mobile computing commodities specifically for or required by the above-mentioned activities is specifically prohibited under this policy, existing desktop and mobile computing commodities purchased under this policy may be used for some of these purposes. For example, existing desktop computers purchased under this policy may be used in the development of a reportable IT project.

Whenever an agency is uncertain as to whether a proposed use of desktop and mobile computing commodities falls within the scope of this policy, it should seek a determination from the Technology Agency.

4989.3 - AGENCY ROLES AND RESPONSIBILITIES

(Revised 03/11)

Management. Day-to-day management responsibility for desktop and mobile computing configurations resides with the manager who has supervisory responsibility for the individual or individuals who use the products. The manager must ensure that the acquisition and use of desktop and mobile computing commodities support the accomplishment of agency objectives and that the individual or individuals who will be using the products will be trained in their use.

Each agency must have a plan for the appropriate application of desktop and mobile computing. Each agency must ensure that its plans are consistent with the agency's information management standards, policies, procedures, and its information technology infrastructure. Agency plans for implementing desktop and mobile computing must not preclude the implementation of other agency applications on the same configuration. Agencies are responsible for establishing desktop and mobile computing standard configurations, ensuring each acquisition made under this policy is consistent with those standards, and accurately tracking the cost associated with such acquisitions. In addition, agencies are responsible for the creation and maintenance of IT assets inventories for commodities purchased under this policy.

Agency management has a responsibility to establish standards of technical assistance in support of such LAN activities such as installation, configuration, problem-determination, maintenance, backup, recovery, and required activities beyond those normally associated with stand-alone personal computers. Agencies are expected to maintain internal processes to ensure that any IT commodities acquired under the authority of this policy are compliant with all applicable hardware, software, and security standards for the agency.

Agency management is responsible for taking appropriate action in the event of employee misuse of desktop and mobile computing technology or employee failure to comply with State and agency policy governing the use of desktop and mobile computing.

Security. Desktop and mobile computing environments owned by state agencies involve the risk of property loss, threats to privacy, and threats to the integrity of state operations. Accordingly, agencies must be in compliance with all applicable provisions of the SAM and must implement appropriate safeguards to secure the agency's desktop and mobile computing infrastructure.

Use of personally owned smartphones is restricted to devices that are compatible with the CA.Mail or the California Email Service, and are consistent with the Statewide Enterprise Architecture.

Current agency Disaster Recovery Plans (DRP) or acceptable DRP certifications must be on file at the Technology Agency. Agencies that do not demonstrate effective compliance with the State's IT security policy

and Disaster Recovery policy are not authorized to make any expenditures for desktop and mobile computing commodities until the agency has complied. See SAM Sections 5300-5399.

Desktop and Mobile Computing Coordinator. In order to ensure ongoing IT asset management practices are followed, agencies employing desktop and mobile computing should designate a unit or individual employee of the agency as the agency's Desktop and Mobile Computing Coordinator or equivalent function. The coordinator must be knowledgeable about (a) desktop and mobile computing configurations; (b) state-level and agency policies for the use of desktop and mobile computing commodities; and (c) the relationship between desktop and mobile computing and other uses of information technology with the agency.

The responsibilities of the coordinator should include:

1. Maintaining current specifications for the agency's desktop and mobile computing commodity standards;
2. Assisting in the completion and review of any DMCP documents if required by the agency's policies and procedures;
3. Coordinating the acquisition of desktop and mobile computing commodities;
4. Informing desktop and mobile computing users of available training and technical support capabilities; and
5. Maintaining continuing liaison with agency IT management to ensure that: (a) proposed desktop and mobile computing applications are consistent with the agency's established information management strategy and information technology infrastructure, (b) desktop and mobile computing configurations can support the implementation of other agency applications.

4989.8 - POLICY COMPLIANCE

(Reviewed 03/11)

If Finance determines that an agency's procedures or practices are not consistent with the Statewide Workgroup Computing Policy or with the agency's own approved policy, delegation of approval authority will be rescinded and the agency will be deemed not to have an approved Workgroup Computing Policy until such time as it can assure Finance of compliance with an approved policy.

5001 - EQUIPMENT ACQUISITION, MAINTENANCE AND DISPOSITION

(Reviewed 03/11)

Information technology equipment that is state-owned will be used as long as its use meets the operational requirements of the user and as long as relative costs versus benefits are favorable. Such equipment will be used, where appropriate and where benefits exceed costs, to replace installed equipment that is on rent or short-term lease anywhere in state government.

The relative merits of all methods of acquisition and maintenance of IT equipment shall be continuously evaluated to assure maximum economic advantages to the state. When selecting equipment, agencies will consider the requirements of interfacing to present systems. Conversion costs must be considered as well as the costs associated with exchanging information among machines. Standard commercially available general purpose IT equipment will be acquired in preference to specially designed and/or special purpose equipment, unless unusual circumstances warrant otherwise.

Duplicate or excess IT equipment will not be acquired as insurance against machine failure or as standby equipment, except in the case of legally required or otherwise necessary full-time or absolute service functions.

The disposition of IT equipment which is excessive to an agency's requirements will be in accordance with the most economical and practical manner for the state as a whole

5010 - POLICY

(Reviewed 03/11)

A uniform method for recording data relating to the repair or maintenance of data processing equipment, software and facilities must be established to prevent degradation in customer and vendor support and excessive maintenance costs. Capturing this data at the time of the incident and ensuring its review by appropriate levels of management is necessary to effectively manage and control the maintenance function.

State agencies should develop a maintenance form which includes essential data pertaining to incidents of repair or maintenance. This essential data required in resolving disputes between the vendor and the state in respect to vendor performance includes:

1. The time at which the vendor maintenance contact was notified by the state;
2. The time at which the vendor maintenance personnel arrived to repair the malfunction;
3. The time at which the component and system were returned to service;
4. A description of the malfunction or incident; and,
5. Signature of the vendor and a representative of the state.

A maintenance form should be prepared whenever a system or any component of a system is inoperative because of the need for equipment, software or facilities repair or maintenance. The form is initiated at the time of the incident and remains open until the problem has been corrected and the component has been returned to service. Copies of completed forms must be maintained by the agency as long as the component is in service or there is a possibility of contractual claims.

5100 - POLICY (Revised 03/11)

The Technology Agency embraces the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS). The ANSI standards are national consensus standards which provide guidance on a variety of issues central to the public and industrial sectors. The FIPS standards are adopted and promulgated under the provision of Public Law 89-306 (Brooks Act) and Part 6 of Title 15, Code of Federal Regulations, and serve to improve the utilization and management of computers and automated data processing in the Federal Government.

State agencies must use the ANSI and FIPS standards in their information management planning and operations. Adoption of these standards will facilitate the interorganizational sharing and exchange of equipment, data, software and personnel. Use of these standards will also facilitate communication (1) among state agencies; (2) between the state and its IT vendors; and (3) between the state and its IT information providers/recipients.

5101 - COMPUTER PROGRAMMING LANGUAGES (Revised 03/11)

The Technology Agency encourages the use of vendor supplied packages versus in-house development whenever vendor supplied packages can be demonstrated to be the most cost beneficial solution to IT project problems or opportunities.

5175.1 - OPERATING SOFTWARE, UTILITIES AND PROGRAMMING AIDS (Reviewed 03/11)

It is state policy that standard, unmodified, vendor-supplied-and-maintained software aids be used in lieu of developing unique programs. The objective is to minimize and control the development of specialized programs that allocate, schedule and control the CPU, memory, peripherals, communication, data storage and retrieval.

5175.2 - APPLICATION PACKAGES (Reviewed 03/11)

It is the state policy that all feasibility studies will address the availability, usability, maintainability and cost

effectiveness of prewritten and tested application programs in lieu of developing major programs in-house. The objective is to minimize the development time and costs of major application programs when such programs are available from other sources.

5179 - COMPLIANCE WITH UNITED STATES POSTAL SERVICE, OPTICAL CHARACTER RECOGNITION GUIDELINES

(Reviewed 03/11)

The United States Postal Service (USPS) has adopted guidelines to allow for optical character recognition of alphanumeric data contained in mailing addresses. Government agencies are strongly encouraged to follow these guidelines as a means of ensuring more efficient and accurate mail processing; more consistent mail delivery; and more stable postal operating costs.

To the extent that it is determined to be cost-effective, agencies must follow the USPS Optical Character Recognition (OCR) guidelines in the design and operation of automated information systems that include preparation of mailing addresses.

The OCR guidelines apply to letter mail within the following dimensions;

1. Height at least 3–1/2" and more than 6–1/8";
2. Length at least 5" and no more than 11–1/2";
3. Thickness at least 0.007" and no more than 0.25"; and,
4. Aspect ratio (length divided by height) of from 1.3 to 2.5.

The details of the guidelines are set forth in the USPS publication, "A Guide to Business Mail Preparation" (Publication 25), which is available without charge. Agencies should contact their USPS Commercial Account Representative to obtain the current edition.

5180 - UNITED STATES POSTAL SERVICE ZIP + 4 GUIDELINES

(Reviewed 03/11)

The USPS offers a reduced postage rate to organizations for first-class mailings that use the 9-digit zip code (ZIP +4) in the mailing address. Both unsorted and sorted mailings are eligible for the reduced rate.

To the extent that it is cost-effective (taking into account the potential postage discount), agencies must provide for ZIP + 4 address coding and sorting of printed addresses in ZIP + 4 order in the design and operation of automated information systems that include preparation of mailing addresses.

There are two preliminary requirements for eligibility for the ZIP + 4 discount;

1. "Machinability," which includes quality of paper stock and adherence to the USPS standards for envelope size; and,
2. Optical Character Recognition (OCR) readability, which consists of adherence to the USPS OCR mailing guidelines.

Detailed specifications for these and other ZIP + 4 requirements are available from the USPS Commercial Account Representative assigned to each agency. Additional information is also contained in Section 324 of the USPS Domestic Mail Manual.
