OFFICE OF THE STATE CIO

IT POLICY LETTER

NUMBER:

ITPL 10-19

SUBJECT:

SMARTPHONE AND OTHER MOBILE COMPUTING DEVICE SECURITY

Emphasis: Securing Remote Access and Information Technology Infrastructure

DATE ISSUED:

DECEMBER 30, 2010

EXPIRES:

Until Rescinded

REFERENCES:

Government Code Sections 11545, 11549, 14200-14203, and 15275-15279
State Administrative Manual Sections 4989.1 and 4989.3
Statewide Information Management Manual Sections 65E and 66A
Department of General Services' 2010 Telework Program Policy and Procedures
Information Technology Policy Letter 10-03

ISSUING AGENCY:

OFFICE OF THE STATE CHIEF INFORMATION OFFICER

DISTRIBUTION

Agency Secretaries
Department Directors
Agency Chief Information Officers
Department Chief Information Officers
Agency Information Security Officers
Information Security Officers
Department Telework Program Managers and Coordinators

PURPOSE

The rapid advancement of smartphone and mobile computing device technology is making their use more attractive to government organizations as budgets continue to shrink and business needs drive increased worker mobility. Accordingly, the purpose of this Information Technology Policy Letter (ITPL) is to:

- Remind state agencies[1] of their responsibilities regarding the secure use of the state's information technology (IT) infrastructure and information assets. This includes:
  - Ensuring the American National Standards Institute (ANSI) standards and Federal Information Processing Standards (FIPS) are used in information management planning and operations.
  - Using the National Institute of Standards and Technology

[1] When capitalized, the term "Agency" refers to one of the state's super Agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. When used in lower case, the term "agency" refers to any office department, board, bureau, commission or other organizational entity within state government. Within this ITPL, "agency" and "department" are used interchangeably.

(NIST) publications referenced in the FIPS.

- Clarify that the Telework and Remote Access Security Standard included as Section 66A of the Statewide Information Management Manual (SIMM) applies to the use and implementation of smartphones and other mobile computing devices.
- Announce the release of the Remote Access Agreement as SIMM Section 65E, and updated content to the Telework and Remote Access Security Standard in SIMM Section 66A.

BACKGROUND

The Office of the State Chief Information Officer (OCIO)[2] has responsibility and authority for the establishment and enforcement of state IT in California State Government. This includes establishing and enforcing the state's IT strategic plans, policies, standards and enterprise architecture. In accordance with Government Code (GC) Sections 11545 and 11549, the Office of Information Security (OIS), within the OCIO, has the authority and responsibility for overseeing state agency compliance with security policies, standards and procedures to ensure the protection of state information assets and citizen data held in trust by state agencies.

In accordance with (GC) Sections 14200 through 14203 and 15275 through 15279, the Department of General Services (DGS) released a new statewide model Telework Program Policy and Procedures. In addition, the OCIO released its companion ITPL 10-03 with emphasis on the importance of securing remote access and IT infrastructure.

As currently released, ITPL 10-03 is applicable to any remote access connection to state IT infrastructure. Accordingly, agencies are advised that the requirements included in ITPL 10-03 include the use smartphone and mobile computing device technology, and are reminded of the standards and implementation guidance published by the NIST and adopted by the state.

POLICY AND PROCESS

Smartphones and other mobile computing devices which are authorized to make a remote connection to a state agency network are subject to all state and departmental policies and standards, including the Telework and Remote Access Security Standard (SIMM 66A), and consistent with the Statewide Enterprise Architecture.

The Remote Access Agreement is added as SIMM 65E, and shall be used in lieu of the DGS' Telework Arrangement agreement when smartphone use and other mobile computing implementations do not fall within the definition of a casual or regular telework arrangement.

Use of personally owned smartphones is restricted to agencies that are utilizing or in migration to the CA.Mail or the California Email Service. Personally owned smartphones must also be compatible with the aforementioned service.

[2] Effective January 1, 2010, the Office of the State Chief Information officer (OCIO) is renamed the California Technology Agency (Technology Agency).

	SAM Section 4989.3, Agency Roles and Responsibilities, will be updated to include the restrictions for using personally owned smartphones.
SAM AND SIMM CHANGES	The SAM Section 4989.1, Definition of Desktop and Mobile Computing, will be updated to include the definitions for Remote Access and for Smartphone. The definition for Desktop and Mobile Computing Commodities will also be updated to include smartphones. In addition, the restrictions for using personally owned smartphones previously discussed will be added to SAM Section 4989.3, Agency Roles and Responsibilities. An advance copy of the SAM updates in included in this ITPL as Attachment A. The SIMM located at http://www.cio.ca.gov/Government/IT_Policy/introduction.html has been updated to include the following changes: • **SIMM Section 66A, Telework and Remote Access Security Standard –** Updated to: (1) Add definitions for Smartphone and for Mobile Computers to the existing Definitions; and (2) Add references to the NIST Special Publications previously discussed. • **SIMM Section 65E, Remote Access Agreement–** Added and to be used in lieu of the DGS' Telework Arrangement agreement when smartphone use and other mobile computing implementations do not fall within the definition of a casual or regular telework arrangement.
ROLES AND RESPONSIBILITIES	Agency Chief Information Officers (CIOs) and Agency Information Security Officers (ISOs) shall ensure departments are in compliance with the smartphone and mobile computing requirements through their department CIOs and ISOs. CIOs and ISOs who are not affiliated with an Agency have the same responsibilities as Agency CIOs and Agency-affiliated department CIOs.
APPLICABLILITY	All state agencies within the Executive Branch that are under the direct authority of the Governor are required to comply with this policy. Other state agencies may voluntarily comply with the policy and may request assistance from the OCIO to do so.
CONTACT	Questions concerning this policy should be directed to the Office of Information Security at (916) 445-5239 or via email to Security@state.ca.gov.
SIGNATURE	/s/ Christy Quinlan, Acting Chief Information Officer State of California

State Administrative Manual Changes

4989.1 DEFINITION OF DESKTOP AND MOBILE COMPUTING
(Revised xx/11)

(Note: The following definitions are being updated or added as indicated by underlined text)

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.

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.

4989.3 AGENCY ROLES AND RESPONSIBILITIES
(Revised xx/10)

(Note: The addition is indicated by underlined text – the remaining text is unchanged)

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 treats 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 OCIO. 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.