OFFICE OF THE STATE CIO

IT POLICY LETTER

	NUMBER: **ITPL 10-03**
SUBJECT: **TELEWORK AND REMOTE ACCESS** **Emphasis: Securing Remote Access and Information Technology Infrastructure**	DATE ISSUED: MARCH 2, 2010 EXPIRES: Until Rescinded
REFERENCES: Governor's Reorganization Plan #1 of 2009 Government Code Sections 11545 et seq, 11549 (a) and (b), 14200-14203 and 15275-15279 State Administrative Manual Section 5340 Statewide Information Management Manual Sections 66A and 70E Department of General Services' 2010 Telework Program Policy and Procedures Transmittal dated January 29, 2010	ISSUING AGENCY: OFFICE OF THE STATE CHIEF INFORMATION OFFICER

DISTRIBUTION

Agency Secretaries
Agency Chief Information Officers
Department Directors
Department Chief Information Officers
Department Information Security Officers

PURPOSE

The purpose of this Information Technology Policy Letter (ITPL) is to:

- Announce the Telework and Remote Access Security Standard included in the State Information Management Manual (SIMM) Section 66A and the Agency Telework and Remote Access Security Compliance Certification included in SIMM Section 70E.
- Require the use of and certification of compliance with this standard by state government agencies[1] and departments.
- Identify changes to the existing State Administrative Manual (SAM) Section 5340 concerning Telework and Remote Access.

[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.

BACKGROUND

Many state agencies provide employees the option to work in a location other than their state owned or leased workplace, such as from home or an alternate work site (e.g., Auditors, Inspectors, and Investigators). Other state agencies, by the nature of the work activity, may require employees to telework from home, alternate work site or from a citizen's place of business. Flexibility of work location has shown to reduce expenses, increase productivity and contribute to employee job satisfaction.

However, the cyber security risks and incidents associated with unmanaged use of remote access and telework arrangements can be just as costly and impact the ability to deliver essential public services. Compliance with security policies and standards will help mitigate both the cyber security and business risk. Accordingly, the Office of the State Chief Information Officer (OCIO) has adopted a mandatory Telework and Remote Access and Security Standard described in the section immediately following.

In a joint effort, the Department of General Services released a new statewide model Telework Program Policy and Procedures. The new policy and procedures, released on January 29, 2010, are available at http://www.dgs.ca.gov/dgs/ProgramsServices/telework.aspx.

POLICY

Agency heads are responsible for ensuring that only authorized users who have been trained regarding their roles and responsibilities, security risks, and the requirements included in the Telework and Remote Access Security Standard SIMM Section 66A, be permitted to telework.

Agency heads shall adopt and ensure the requirements in the Telework and Remote Access Security Standard, included in SIMM Section 66A, are implemented. In addition, agency heads shall certify their agency's compliance with the standard. Those agencies that have existing Telework and Remote Access programs in place which do not meet this standard must certify as to their plan and timeline for achieving compliance.

Agency heads shall complete and submit the Agency Telework and Remote Access Security Compliance Certification form included in SIMM Section 70E to the OCIO-Office of Information Security (OIS) **no later than July 1, 2010,** and annually thereafter beginning January 31, 2011.

When the development of an agency plan is necessary to achieve compliance with this standard, the plan shall be held by the agency and made available for review by the OCIO-OIS upon request.

APPLICABILITY	This policy establishes requirements, by reference to SIMM 66A and SIMM 70E, in the SAM Section 5340 for all state agencies, and is applicable to agency heads, agency management, agency IT administrators, and telework users.
SAM/SIMM UPDATES	An advanced copy of the updated SAM Section 5340 is included in Attachment A. Updates to SIMM Sections 66A and 70E are available on the OCIO's Web site at http://www.cio.ca.gov/Government/IT_Policy/SIMM.html.
DEFINITIONS	**Telework** – An arrangement in which an employee regularly performs officially assigned duties at home or an alternate work site. **Remote Access** – The connection of an information asset from an off-site location to an information asset on state IT infrastructure.
CONTACT	Questions concerning this policy should be directed to your CIO, your Chief Information Security Officer, or the OCIO-OIS. Contacts for the OCIO-OIS can be reached at (916) 445-5239 or security@state.ca.gov.
SIGNATURE	/s/ _____ Teri Takai, Chief Information Officer State of California

SAM - Chapter 5300

5340 ACCESS CONTROL
(Revised 2/10)

Agency management is responsible for ensuring the appropriate physical, technical, and administrative controls are in place to support proper access to agency information assets. These controls must be based on both business and security requirements to prevent and detect unauthorized access, and must, at a minimum, include the following controls

1. Mobile, telework and remote access controls include, but are not limited to the following:

    a. Compliance with the Telework and Remote Access Security Standard (SIMM 66A).

    b. Certifying compliance with the Telework and Remote Access Security Standard (SIMM 66A) by submission of the Agency Telework and Remote Access Security Compliance Certification (SIMM 70E).

    c. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information, and information necessary for the support of agency critical applications.

    d. Periodically changing dial-up access telephone numbers.

    e. Auditing usage of dial-up communications and Internet access for security violations.

AUTHORITY STANDARDS GUIDANCE FORMS TOOLS