CALIFORNIA TECHNOLOGY AGENCY **TECHNOLOGY LETTER**	NUMBER: **TL 12-15**	DATE ISSUED: **DECEMBER 6, 2012**
SUBJECT: **ENCRYPTING MAINFRAME AND SERVER TAPES:** Require encryption of personal, sensitive or confidential information	REFERENCES: State Administrative Manual Section 5345.2 Statewide Information Management Manual 70C	

BACKGROUND

State Administrative Manual (SAM) Section 5345.2 includes a requirement that all state entities[1] encrypt personal, sensitive, and confidential information when it is stored on portable electronic storage media, such as CDs and thumb drives. SAM Section 5345.2 also requires encryption of portable computing devices including, but not limited to, laptop and notebook computers. Mainframe and server tapes are currently excluded from the encryption requirement because, when the policy was last updated in 2009, encrypting mainframe and server tapes was costly and difficult for most organizations. Since 2009, technology has advanced, reducing the cost and making tape encryption feasible. In addition, alternative transport and back-up solutions, such as Secure File Transfer, exist today which do not require the physical transport of mainframe and server data on tape media.

PURPOSE

The purpose of this Technology Letter (TL) is to:

- Remove the exclusion in SAM Section 5345.2 to encrypt mainframe and server tapes that contain personal, sensitive or confidential information.
- Allow state entities to use compensating security control alternatives to encryption that are approved in writing by the agency Information Security Officer, after a thorough risk analysis.
- Modify the Statewide Information Management Manual (SIMM) 70C form to require that the department head certify compliance with this policy change.
- Add examples of "portable electronic storage media" and "portable computing devices" that are subject to SAM Section 5345.2.

An advance copy of the changes to SAM Section 5345.2 and SIMM 70C are included as Attachment A. SIMM has been updated and the SAM section will be updated at the first available opportunity.

[1] "State entity" refers to any office, department, board, bureau, commission, or other organizational entity in state government, including Agencies such as the Environmental Protection Agency or the Health and Human Services Agency.

PROCESS

State entities with mainframe or server tapes that store personal, sensitive or confidential information as defined by SAM Section 5345.2, must encrypt those tapes or use approved compensating security control(s).

Alternative measures must be reviewed and judged to provide equivalent or comparable protection as encryption. Any alternative must be approved in writing by the agency Information Security Officer (ISO), after a thorough risk analysis. Longstanding policy and process for conducting a thorough risk analysis are located in SAM Section 5305.1.

State entities must annually certify the status of their compliance with requirements prescribed in SAM Chapter 5300 using the SIMM 70C form. In accordance with this annual filing and its instructions, any state entity not fully compliant with this policy by their next submission shall include a remediation plan along with the timeline indicating when the requirement will be met.

QUESTIONS

Questions should be directed to the Office of Information Security (OIS) at (916) 445-5239 or Security@state.ca.gov.

SIGNATURE

/s/

Carlos Ramos, Secretary

California Technology Agency

STATE ADMINISTRATIVE MANUAL EXCERPTS

[Note: Text to be deleted is shown in strikethrough; text to be added is underlined.]

5345.2 CRYPTOGRAPHY

(Revised 12/12)

Encryption, or approved compensating security control(s)~~equally effective measures~~, is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs, DVDs, tapes, portable hard drives, and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers, netbooks, tablets, and smart phones). ~~This policy does not apply to mainframe and server tapes.~~

For the purpose of this policy, the terms "confidential information" and "sensitive information" are defined in SAM Sections 5320.5, and, "personal information" is defined in three categories as follows:

1. Notice-triggering information (Civil Code Section 1798.29).

2. Protected health information (45 C.F.R. Section 160.103).

3. Electronic health information (45 C.F.R. Section 160.103).

Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the agency ISO, after a thorough risk analysis. (See SAM Section 5305.1).

STATEWIDE INFORMATION MANUAL CHANGE

[Note: Text to be deleted is shown in strikethrough; text to be added is underlined.]

DATE: _____

TO: California Technology Agency
Office of Information Security
Attn: Security Compliance Reporting
P.O. Box 1810, Mail Stop Y-12
Rancho Cordova, CA 95741

FROM: _____ _____
Org Code – As identified in the Uniform Codes Manual | Name of Organization

SUBJECT: Agency Risk Management and Privacy Program Compliance Certification

As specified in State Administrative Manual (SAM) Section 5315.1, "The agency director has ultimate responsibility for information technology security, risk management, and privacy within the agency." As the Secretary/Director (*or equivalent head of the agency*) or the Secretary/Director's designee, I certify that our organization is in compliance with requirements prescribed in SAM Sections 5300-5399, California Government Code Sections 11549.3 (b), and 11019.9 as follows (*select one*):

☐ Our organization has implemented a fully developed Risk Management and Privacy Program that complies with all policy requirements in SAM Sections 5300-5399 including:

- A risk management program that includes the identification and prioritization of critical information technology applications, ongoing risk assessment, risk analysis, risk acceptance and risk communication. See SAM Section 5305.
- Policies that establish and maintain a standard of due care to prevent misuse or loss of state information assets. See SAM Section 5310.
- Assigned management responsibilities for information technology risk management, including the appointment of an Information Security Officer. See SAM Section 5315.
- Identification and classification of all records and identification of ownership responsibilities for all records, files and data bases to ensure the integrity and security of agency information assets. See SAM Section 5320.
- Assigned security roles and responsibilities for employees, contractors and third party users, and personnel management practices that include annual security and privacy training for all employees, contractors, and other individuals who have access to personal, confidential or sensitive information, acknowledgement of their understanding of the consequences of violating agency information privacy and security policies, and termination procedures to ensure assets are not accessible to former employees. See SAM Section 5325.
- Physical security practices for each facility to prevent unauthorized physical access, damage, or interruption to agency assets. See SAM Section 5330.

- Identification and documentation of appropriate practices to ensure the integrity and security of agency information assets that include the agency ISO's approval of proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data before implementation. See SAM Section 5335.

- Appropriate physical, technical, and administrative controls are in place to support proper access to agency information assets that include business and security requirements to prevent and detect unauthorized access. These controls provide full compliance with the Telework and Remote Access Security Standard as described in SIMM66A. See SAM Section 5340.
- **Information on portable electronic storage media, including mainframe and server tapes, is encrypted or is protected by approved compensating security controls.** See SAM Section 5342.2.
- Security practices throughout the System Development Life Cycle for the integrity and security of information assets that include use of secure coding standards, and separation of development and testing functions. This section also includes software licensing integrity practices and encryption of portable electronic storage media. See SAM Section 5345.
- An Incident Management program that provides for timely reporting, investigation, response, and recovery from incidents; and, when required, notification to individuals. See SAM Section 5350.
- An agency Disaster Recovery Plan that meets the Statewide Information Management Manual (SIMM) 65A requirements. See SAM Section 5355.

☐ Our organization has NOT yet implemented all required components. We have attached our remediation plan that identifies the non-compliant components along with timelines indicating when our organization will meet these requirements.

I hereby further certify our organization has undergone a comprehensive enterprise-wide risk assessment and analysis in the past two-years, which at a minimum, was designed to measure our organization's compliance with the legal and policy requirements outlined in SAM Sections 5300-5399. The date of our agency's last comprehensive enterprise-wide risk assessment was

_____.

The status of our remediation activity from the last comprehensive assessment and analysis is as follows (*select one*):

☐ No remediation activity was identified through the assessment.
☐ Remediation activity was identified, prioritized, and will be complete by _____.
☐ All remediation activity identified through the assessment is complete.

For additional information about this submission please contact:

Name	at Telephone Number	or Email

Printed Name of Secretary/Director or Designee	Signature of Secretary/Director or Designee	Date