BUDGET LETTER

SUBJECT: INFORMATION TECHNOLOGY SECURITY POLICY – INFORMATION SECURITY NOTIFICATION AND REPORTING	**NUMBER:** 06-34
	DATE ISSUED: December 7, 2006
REFERENCES: GOVERNMENT CODE 11019.9, CIVIL CODE 1798 ET SEQ., MANAGEMENT MEMO 06-12, STATE ADMINISTRATIVE MANUAL SECTIONS 4841, 4841.1, 4845 AND STATEWIDE INFORMATION MANAGEMENT MANUAL SECTIONS 65B, 65C, AND 70C	**SUPERSEDES:**

TO: Agency Secretaries
Agency Information Officers
Department Directors
Department Budget Officers
Department Chief Information Officers
Department Information Security Officers
Department Privacy Officers
Department Accounting Officers
Department of Finance Budget Staff

FROM: DEPARTMENT OF FINANCE

BACKGROUND

The Department of Finance (Finance) is responsible for establishing the state's information security policies and activities, and for information security oversight. This BL revises the policies for information security incident notification and reporting requirements. The word "agency" is used in the policy and within this BL to be consistent with the definition in State Administrative Manual (SAM) Section 4819.2: "When used in lower case, (agency) refers to any office, department, board, bureau, commission or other organizational entity within state government."

The recent release of Management Memo 06-12, regarding the protection of information assets, has warranted changes and updates in current policy regarding information security and privacy programs, including a requirement for an annual training component to provide ongoing education for all employees and contractors who handle personal, sensitive, or confidential information. Additionally, the notification and reporting requirements for information security incidents have been updated to include the recent changes identified in the Management Memo.

POLICY CHANGES OR ENHANCEMENTS

Advance copies of the policy changes or enhancements to SAM and the Statewide Information Management Manual (SIMM) are included as the following Attachments:

Attachment 1 – SAM Section 4841 - Agency Responsibilities

- Added item number 6 requiring agencies to maintain a privacy and security program, including annual training for employees.

Attachment 2 – SAM Section 4841.1 – Agency Management Responsibilities
- Clarified the Technical Management section.
- Modified the Program Management section to include privacy responsibilities.

Attachment 3 – SAM Section 4845 – Agency Information Security Reporting Requirements
- Added a requirement for reporting incidents involving paper, removed the dollar threshold for reporting equipment incidents, and clarified the requirements for incident reporting and notification to provide responsibilities and criteria for reporting incidents.

Attachment 4 – Agency Information Security Incident Notification and Reporting Instructions (SIMM 65B)
- The process for agencies to follow in reporting incidents was previously included in SAM Section 4845. This process was removed from policy and placed in SIMM 65B as instructions agencies must follow to report information security incidents.

Attachment 5 – Agency Information Security Incident Report (SIMM 65C)
- The Report has been renumbered from SIMM 140 to SIMM 65C to be more consistent with the Instructions. A new field is added for agencies to include their organization code, as identified in the Uniform Codes Manual. The content of the report has not changed.

Attachment 6 – Agency Risk Management and Privacy Program Compliance Certification (SIMM 70C)
- The Risk Management Certification has been renamed to the Agency Risk Management and Privacy Program Compliance Certification (SIMM 70C). This Certification now requires agency directors to identify the individual who oversees their privacy program and to certify they have an ongoing annual training program in place or indicate when they will have the training program in place. Additionally, a new field is added for agencies to include their organization code, as identified in the Uniform Codes Manual.

All changes described in this BL are effective immediately.

CONTACTS AND QUESTIONS

You may call the State Information Security Office at (916) 445-5239 if you have questions about this BL.

/s/ Fred Klass

Fred Klass
Program Budget Manager

Attachments

4841 AGENCY RESPONSIBILITIES

(Revised 12/06)

Each agency must provide for the proper use and protection of its information assets. Accordingly, each agency must perform the following:

1. Assign management responsibilities for information technology risk management, including the appointment of an Information Security Officer. See SAM Section 4841.1.

2. Provide for the integrity and security of automated information, produced or used in the course of agency operations. See SAM Sections 4841.2 through 4841.7.

3. Provide for the security of information technology facilities, software, and equipment utilized for automated information processing. See SAM Section 4842.2.

4. Establish and maintain an information technology risk management program, including a risk analysis process. See SAM Section 4842.

5. Prepare and maintain an agency Operational Recovery Plan. See SAM Section 4843.1.

6. Maintain an ongoing privacy and security program, as outlined in Government Code 11019.9 and Civil Code 1798 et seq., including an annual training component for existing employees and training for new employees.

7. Comply with the state audit requirements relating to the integrity of information assets.

8. Comply with state reporting requirements. See SAM Section 4845.

4841.1 AGENCY MANAGEMENT RESPONSIBILITIES
(Revised 12/06)

Executive Management–The agency director has ultimate responsibility for information technology security, privacy and risk management within the agency. On an annual basis the Director of each state agency must submit a Department Designation Letter (SIMM Section 70) designating critical personnel. See SAM Section 4845. Each year, the agency director must certify that the agency is in compliance with state policy governing information technology security, risk management, and privacy program by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70). See SAM Section 4842 and 4845. The Director must also transmit each year an updated copy of the agency's Operational Recovery Plan or Operational Recovery Plan Certification (SIMM Section 70) to the Department of Finance. See SAM Sections 4843.1 and 4845.

Information Security Officer–The Information Security Officer (ISO) is required to oversee agency compliance with policies and procedures regarding the security of information assets. The ISO must be directly responsible to the agency director for this purpose and be of a sufficiently high-level classification that he or she can execute the responsibilities of the office in an effective and independent manner. It is acceptable to create this reporting relationship on a functional basis rather than reorganize the department. To avoid conflicts of interest, the ISO (for agencies other than state data centers) should not have direct responsibility for information processing, technology operations, or for agency programs that employ confidential information.

Operational Recovery Coordinator-Each agency must designate an Operational Recovery Coordinator to represent the agency in the event of a disaster or other event resulting in the severe loss of IT systems capability. The designated individual must have sufficient knowledge of information management and information technology within the agency to work effectively with the data centers and vendors in re-establishing information processing and telecommunications services after an event has occurred. The name, title, business address, and phone number of the coordinator must be submitted to the Department of Finance with the agency's Operational Recovery Plan and annual Department Designation Letter (SIMM Section 70), as appropriate. See SAM Section 4845.

Technical Management–Agency information technology management is responsible for (1) implementing the necessary technical means to preserve the security, privacy, and integrity of the agency's information assets and manage the risks associated with those assets and (2) acting as a custodian of information per SAM Section 4841.6.

Program Management–Agency program managers are responsible (1) for specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) for ensuring that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.

The establishment of positions to meet agency information security responsibilities must be justified in accordance with established personnel and budgetary requirements.

4845 AGENCY INFORMATION SECURITY REPORTING REQUIREMENTS
(Revised 12/06)

All agencies must adhere to the following Information Security Reporting Requirements:

1. Security Incident Reporting
All agencies are required to report information security incidents according to the security reporting requirements that follow.

a. Agency Responsibilities – Agency management must promptly investigate incidents. Upon discovery of any incident that meets the defined criteria below, agencies must immediately report the incident following the Agency Information Security Incident Notification and Reporting Instructions found in SIMM Section 65B and in this policy.

Any incident involving personal identifying information may require the agency to notify the affected individuals.

b. Criteria for Reporting Incidents - Incidents reported to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) include, but are not limited to, the following:

- **State Data (includes electronic, paper, or any other medium)**
  - Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal. (See SAM Section 4841.3)
  - Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
  - Deliberate or accidental distribution or release of personal information by an agency, its employee(s), or it contractor(s) in a manner not in accordance with law or policy.
  - Intentional noncompliance by the custodian of information with his/her responsibilities. (See SAM Section 4841.6)

- **Inappropriate Use & Unauthorized Access -** This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.

- **Equipment** - Theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

- **Computer Crime** - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502. See SAM Section 4840.4, for a definition of an information asset.

- **Any other incidents that violate agency policy.**

c. **Incident Follow-up Report** - Each agency having ownership responsibility for the asset (SAM Section 4841.4) must complete an Agency Information Security Incident Report (SIMM Section 65C, formally SIMM Section 140) for each incident. The report, signed by the agency director and Information Security Officer, must be submitted to the Department of Finance (Finance) within ten (10) business days from the date of notification.

   Additional reporting may be necessary for agencies that must adhere to Health Insurance Portability and Accountability Act (HIPAA) requirements. Refer to the California Office of HIPAA Implementation (CalOHI) Policy Memorandum 2006-77 which can be found on the CalOHI website at www.ohi.ca.gov.

   Finance may require that the agency provide additional information in conjunction with its assessment of the incident.

2. **Designation of Information Security Officer and Operational Recovery Coordinator** – Due by January 31 of each year, or as designee changes occur. The director of each agency must designate and provide contact information for the agency's Information Security Officer (ISO) and the Operational Recovery Coordinator using the Department Designation Letter (SIMM Section 70A). Upon the designation of a new ISO and/or Operational Recovery Coordinator, the agency must submit an updated Department Designation Letter to Finance within ten (10) business days. See SAM Section 4841.1.

3. **Agency Risk Management and Privacy Program Compliance Certification – Due by** January 31 of each year. The director of each agency must certify that the agency is in compliance with state policy governing information technology risk management and privacy program compliance by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). See SAM Section 4842.1. Per Government Code Section 11019.9, agencies are required to maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Civil Code section 1798 et seq.) that includes, but is not limited to, assigning a designated individual to oversee the program.

4. **Operational Recovery**
   All state agencies are required to provide the following:

   a. **Designation of Operational Recovery Coordinator – See number 2 above regarding** requirements for agencies to follow in designating their Operational Recovery Coordinator.

   b. **Operational Recovery Plan** – Each agency must file a copy of its Operational Recovery Plan (ORP) with the Department of Finance by the due date outlined in the Operational Recovery Plan Quarterly Reporting Schedule (SIMM Section 05). If the agency employs the services of a state data center, it must also provide the data center with a copy of its plan or subset of the relevant recovery information from the agency's ORP. See SAM Section 4843.1.

   c. **Operational Recovery Plan Certification** – An Operational Recovery Plan Certification (SIMM 70B) may be filed in place of a full ORP by the due date outlined in the Operational Recovery Plan Quarterly Reporting Schedule (SIMM Section 05), if specific conditions exist. See SAM Section 4843.1.

AGENCY INFORMATION SECURITY INCIDENT NOTIFICATION AND REPORTING INSTRUCTIONS

Incident Notification

State policy requires agencies to follow this notification process when information security incidents described in SAM Section 4845 occur. Typically, it is each agency's Information Security Officer's (ISO) responsibility to notify the proper authorities following these steps:

1. **Responsibility of the agency ISO or backup ISO:**
   Call (916) 657–8287 immediately to report the incident. This number is a 24-hour phone line at the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC). The CHP contact will require specific information about the incident and will forward that information to the State Information Security Office (in the Department of Finance) and to the Computer Crimes Investigation Unit (CCIU at the CHP).

2. Guidance for reporting the incident can be located on CHP's Web site at www.chp.ca.gov under "Computer Crime Reporting for State Agencies." If available, the following information should be gathered before calling ENTAC:

   - Name and address of the reporting agency.
   - Name, address, e-mail address, and phone number(s) of the reporting person.
   - Name, address, e-mail address, and phone number(s) of the ISO.
   - Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
   - Description of the incident.
   - Date and time the incident occurred.
   - Date and time the incident was discovered.
   - Make / model of the affected computer(s).
   - IP address of the affected computer(s).
   - Assigned name of the affected computer(s).
   - Operating system of the affected computer(s).
   - Location of the affected computer(s).

3. During this notification process, it is important to report if the incident involves personally identifiable information, such as notice-triggering personal information, protected health information, or electronic health information, as defined in SAM Section 4841.3.

4. The CCIU, the State Information Security Office, and Office of Privacy Protection may contact the agency for additional information or further investigation.

Incident Reporting

An Agency Information Security Incident Report (SIMM 65C) outlining the details of the incident and corrective action to be taken must be completed and forwarded to the Department of Finance, State Information Security Office within 10 business days following the incident per SAM Section 4845. The report must be signed by the agency director and the Information Security Officer.

Incident reports should be mailed to:

Department of Finance (Finance)
915 L Street, 6th Floor
Sacramento, CA 95814
Attention: State Information Security Office

Questions may be directed to security@dof.ca.gov or by calling (916) 445-5239.

AGENCY INFORMATION SECURITY INCIDENT REPORT

Instructions: Following the requirements outlined in State Administrative Manual (SAM) Section 4845 and guidance outlined in Statewide Information Management Manual (SIMM) Section 65B, complete this form, and forward it the address located at the bottom of the form within ten (10) business days from the date of notification.

Org Code :
(as identified in the Uniform Codes Manual) _____

Agency: _____

Agency Information Security Officer: _____

Address: _____

Telephone: _____

Date Incident Occurred: _____ Time Incident Occurred: _____

Incident Reported to: _____
(California Highway Patrol, Attorney General, District Attorney, Other)

Date Reported: _____ Contact: _____ Telephone: _____

Description of Incident:

Estimated Cost of Incident $ _____

Factors Included in Cost Estimate:

Corrective Actions Taken to Prevent Future Occurrences:

Estimated Cost of Corrective Actions: $ _____

Factors Included in Cost Estimate:

Have those responsible for the incident been identified? _____

If so, how many individuals were involved? _____

Were state employees involved? _____

Will criminal charges be filed? _____

If so, under what code sections? _____

What other actions will be taken against those who were responsible for the incident?

Prepared by: _____ Date Prepared: _____

Title: _____ Telephone: _____

SIGNATURES:

_____ _____
(Agency Information Security Officer) (Date)

_____ _____
(Agency Director) (Date)

Mail this completed report to:
Department of Finance
915 L Street, 6th Floor
Sacramento, CA 95814
Attention: State Information Security Office

AGENCY RISK MANAGEMENT AND PRIVACY PROGRAM COMPLIANCE CERTIFICATION

DATE: _____

TO: Department of Finance (Finance)
915 L Street, 6th Floor
Sacramento, CA 95814
Attention: State Information Security Office

FROM: _____
(Org Code - as identified in the Uniform Codes Manual) (Name of Agency)

SUBJECT: ANNUAL AGENCY RISK MANAGEMENT AND PRIVACY PROGRAM COMPLIANCE CERTIFICATION

I certify that I am the Director or Director's designee and, as prescribed in State Administrative Manual (SAM) Section 4842 and California Government Code Section 11019.9, I certify that this agency is in compliance with the following:

- State policy governing information technology risk management as specified in SAM Section 4842.2.
- The privacy program mandates identified in Government Code Section 11019.9 and the Information Practices Act (Civil Code Section 1798 et seq.).
- Ensuring the privacy program includes an annual training component for all employees, contractors, and other individuals who have access to personal, confidential or sensitive information and their understanding of the consequences of violating agency information privacy and security policies.
- Designated individual assigned to oversee my agency's privacy program.

_____
(Name) (Telephone Number and/or E-Mail)

Check one:

☐ Our agency currently has an annual training component in place.

☐ Our agency will have an annual training component in place by
(Date)

Please contact: _____ At _____
(Name) (Telephone Number and/or E-Mail)
for additional information.

_____/_____/_____ _____
(Date) (Signature of Director or Designee)