BUDGET LETTER

NUMBER:	BL 03-03
SUBJECT: NOTIFICATION OF INFORMATION TECHNOLOGY INCIDENTS AND COMPUTER CRIMES	**DATE ISSUED:** February 4, 2003
REFERENCES: BL 02-29; SAM SECTION 4845; SIMM SECTION 140; CALIFORNIA PENAL CODE SECTION 502	**SUPERSEDES:**

TO: Agency Secretaries
Agency Information Officers
Department Directors
Department Information Security Officers
Department Chief Information Officers
Departmental Budget Officers

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your Departmental Information Security Officers and Departmental Chief Information Officers even though Finance Technology Investment Review Unit and Technology Oversight and Security Unit will also distribute separately.

BACKGROUND:

The Department of Finance (Finance) is responsible for establishing the framework for the State's information technology (IT) security policies and activities, and for IT security oversight. Finance is responsible for consulting with and supporting departments during and following incidents, and collecting and cataloging security incident information.

In conformance with State law, the California Highway Patrol (CHP) is responsible for law enforcement related to criminal IT security intrusions and will conduct criminal investigations when security incidents occur that warrant this action.

Budget Letter 02-29 and the State Administrative Manual (SAM) Section 4845 require that State departments contact Finance and/or the CHP when specific security incidents and/or computer crimes occur.

These contact points have now been consolidated. The CHP will receive all security incident and computer crime notifications and will notify Finance of all security matters. The CHP's Emergency Notification and Tactical Alert Center (ENTAC) will serve as the incident notification center. CHP ENTAC personnel are available to receive these notifications 24 hours a day, 7 days a week.

CHANGE IN NOTIFICATION PROTOCOL:

Effective February 1, 2003, departments shall notify the CHP ENTAC at (916) 657-8287 about all IT security incidents and computer-related crimes immediately upon discovery of the incidents. A list of incidents that require notification follows this section. This requirement supersedes the existing Budget Letter 02-29 requirement to notify Finance within two hours of security incidents.

Notifications by departments should follow their established internal departmental notification protocols, and shall involve the department's Information Security Officer, or his/her designee. Department representatives making this notification to CHP ENTAC should be prepared to provide the information listed in Attachment A. When CHP ENTAC receives an incident notification, it will notify Finance.

Consistent with Finance's IT security oversight role, Finance will follow up on reports of security incidents, provide advice and assistance, and will handle communications, as needed, including to other departments, control agencies, and the State Chief Information Officer. The CHP will continue to investigate computer crime and will investigate security incidents that may constitute criminal acts.

Please note that a written report is still required to be sent to the Finance Technology Oversight and Security Unit (TOSU) ten working days after the discovery of an incident, as described in SAM Section 4845 (Attachment B). The report is to be signed by the department's director and Information Security Officer and sent to Finance, Attention TOSU Security Unit. The format for the Security Incident Report is provided in the State Information Management Manual (SIMM), Section 140 (Attachment B).

Finance security staff will work with departments in resolving security issues and, in conjunction with a security advisory group, will advise and work with departments that need assistance with the incident resolution and follow-up process.

INCIDENTS THAT REQUIRE NOTIFICATION:

Notification is required for computer crimes and IT security incidents. Details are in SAM and in California Penal Code, with a summary provided below:

- State-owned or State-managed data, without authorization, was damaged, destroyed, deleted, shared, altered, or copied, or used for non-State business. This includes computer documentation and configuration information, as well as electronic and non-electronic data and reports.
- Unauthorized parties accessed one or more State computers, computer systems, or computer networks. This includes deliberate and unauthorized uses of state-owned computer services, as well as "hacker attacks."
- Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer software or computer programs which reside or exist internal or external to a State computer, computer system, or computer network.
- Disruption of state computer services or denial of computer services occurs in a manner that appears to have been caused by deliberate and unauthorized acts.
- A contaminant was introduced into any State computer, computer system, or computer network. This includes, but is not limited to viruses, Trojans, worms, and other types of malicious attacks.
- Internet domain names and/or user account names have been used without permission in connection with the sending of one or more electronic mail messages, and thereby caused damage to a state computer, computer system, or computer network, or misrepresented the state or state employees in electronic communications.
- Damage or destruction of state information processing facilities has occurred.
- Physical intrusions into state facilities have occurred that may have resulted in compromise of state data or computer systems.

Additionally, SAM Section 4845 (Attachment C) and Penal Code Section 502 (c) (Attachment D) contain detailed definitions of IT security incidents and/or computer-related crimes.

Questions regarding this Budget Letter may be directed to the Finance TOSU office at (916) 445-3137.

/s/ KATHRYN RADTKEY-GAITHER

KATHRYN RADTKEY-GAITHER
Assistant Director

Attachments

Reporting Security Incidents and Computer-Related Crimes

Please provide the following information when reporting IT security incidents and computer-related crimes to the CHP 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 Information Security Officer (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).

DEPARTMENT OF FINANCE
SECURITY INCIDENT REPORT

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)

State Administrative Manual Section 4845

Each agency having ownership responsibility for information (SAM Section 4841.4) must complete an Information Security Incident Report. The report, signed by the agency director and Information Security Officer, must be submitted to the Department of Finance within ten working days of the agency's becoming aware of an incident involving one or more of the following:

1. Unauthorized intentional release, modification, or destruction of confidential or sensitive information or the theft of such information, including information stolen in conjunction with the theft of a computer or data storage device;
2. Use of a State information asset in commission of a crime;
3. Tampering, interference, damage, or unauthorized access to computer data and computer systems as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502;
4. Intentional non-compliance by the custodian of information with their responsibilities as defined in SAM Section 4841.6; or
5. Intentional damage or destruction of state information assets, or the theft of such assets, with an estimated value in excess of $2,500.

The State Information Management Manual (SIMM) Section 140 provides the format for the incident report. Finance may require that the agency provide additional information in conjunction with its assessment of the incident.

California Penal Code 502 (c)

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.