BUDGET LETTER

SUBJECT: SAFEGUARDS FOR FIREWALLS AND SERVERS	**NUMBER:** 03-11
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTION 4841.2	**DATE ISSUED:** May 13, 2003
	SUPERSEDES:

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

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your department's Information Security Officers (ISOs) and department's Chief Information Officers (CIOs) even though the Finance State ISO Office will also distribute it separately to the ISOs and CIOs on the current contact list.

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. This is an advisory BL, to point out some key policies and practices that should be prominent components of your department's IT security program.

To ensure that your department has established appropriate policies and is using standard practices for these key areas of information security, departments should examine their existing policies and practices in the areas listed below. Departments that do not have these policies already in place should consider adding them. This is an opportunity for you to implement important industry standard policies and improve the effectiveness of your security program.

IMPORTANT POLICIES AND PRACTICES

As described in the State Administrative Manual Section 4841.2, each department must have a set of IT security policies in place. The following policy areas represent key elements of a strong department security program. In addition to well-defined policies, it is important that departments have practices in place to support the policies. Because the items listed below are inter-related, your department's policies and practices in this area should be consistent with each other, should consistently address developing and maintaining documentation, and should include appropriate change tracking practices.

- **Technology upgrade policy** should include, but not be limited to, operating system upgrades on servers, routers, and firewalls. The policy should address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
- **Security patches and security upgrade policy** should include, but not be limited to, servers, routers, and firewalls. The policy should address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.

- **Firewall configuration policy** should require creation and documentation of a baseline configuration for each firewall, updating documentation for all authorized changes, and should require periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
- **Server configuration policy** should clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy should require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodically checking of the configuration to ensure that it has not changed during software modifications or re-booting of the equipment.
- **Server hardening policy** should cover all servers throughout the department, even those that fall outside of the jurisdiction of the department's IT area. The policy should include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy should address and be consistent with your department's policy for managing security upgrades and security patches. This will ensure that information about new vulnerabilities results in appropriate decisions and actions about server hardening.

Finance will soon release a self-assessment survey to all departments asking that they identify whether they are taking appropriate no-cost and low cost measures to manage information security risk and whether they have appropriate policies and practices in place.

CONTACTS AND QUESTIONS

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

/s/ KATHRYN RADTKEY-GAITHER

KATHRYN RADTKEY-GAITHER
Assistant Director

Upcoming Budget Letters

- Cooperative Work Agreements
- Office Revolving Fund Disbursements