BUDGET LETTER

	NUMBER: 02-29
SUBJECT: INFORMATION SECURITY CONTROLS	**DATE ISSUED:** Sept. 12, 2002
REFERENCES: STATE ADMINISTRATIVE MANUAL 4840-4845	**SUPERSEDES:**

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

FROM: DEPARTMENT OF FINANCE

Note: Please forward a copy of this Budget Letter (BL) to your department's/agency's Chief Information Officer (CIO).

Information security is a critical priority to ensure the integrity of and protect the State's significant investment in information assets. This letter highlights and reminds agencies ("agency" refers to agencies, departments, boards, and commissions) of some of the most critical controls, which can help to protect systems and data.

Agencies should already have in place basic controls including those for physical security and data access, and procedures to assess security vulnerabilities. However, this listing outlines the most critically required controls and the timeframe for agencies to ensure they are in place and operational. As these controls reflect existing requirements, agencies should not incur new costs. Additionally, specific references to resources that provide a broad array of information including ways to protect against Internet security vulnerabilities are provided.

By October 15, 2002, agencies need to verify that the following controls are in place:

1. An Information Security Officer (ISO) has been appointed as required by Section 4841.1 of the State Administrative Manual (SAM).

2. Regular system backups of appropriate systems with at least one copy of the backup media securely stored at an offsite location. Data restore tests are conducted periodically.

3. Procedures to evaluate and apply appropriate vendor-supplied fixes (software and patches) necessary to mitigate security vulnerabilities are in place. The procedures should provide for testing updates and patches prior to installation.

4. Appropriate authentication procedures (user IDs, passwords, etc.) for user accounts and access to systems and data files are implemented.

5. Anti-virus software, to adequately protect the mail gateways, servers, and workstations, is installed and maintained.

6. Unneeded services and software on routers, ports, servers, and network devices have been removed.

7. Procedures are established to report information security incidents (SAM Section 4845) to the Department of Finance, Technology Oversight and Security Unit (Finance/TOSU) **within two hours of becoming aware of the incident** (this is a policy change that will be reflected in the January 2003 update of the State Administrative Manual, but is effective now).

   - During normal business hours contact Finance/TOSU at (888) 918-1062.
   - Outside of normal business hours contact the Teale Data Center Help Desk at (916) 464-4311.

   Remember, also, to *promptly* notify the California Highway Patrol and other appropriate law enforcement agencies if a security incident may constitute a criminal act.

By October 15, 2002, agencies must provide the following information:

- A list of all internet-based systems and applications that are not located behind a firewall. Submit this list to Finance/TOSU, attention Patricia Kuhar, marked “confidential.”

By the date published on the attached “Agency Schedule” the agency should:

- Update the IT Operational Recovery Plan (ORP) so that it is up-to-date, with a test plan, and ready for implementation.

There are numerous references available to agencies to assist them in the establishment of policies, procedures, and controls to protect the confidentiality, integrity and availability of their networks, systems, and databases. Three specific references are listed below.

State Administrative Manual Sections 4840 et.al.

These Sections contain the State’s long-standing security and risk management policies. It is available at: **http://sam.dgs.ca.gov**. Subjects include the duties of information security officers, classification of information, risk management/risk analysis, and operational recovery planning.

Practices for Securing Critical Information Assets

This is a publication of the U.S. Critical Infrastructure Assurance Office. It is available at **http://www.ciao.gov**. Subjects include information security policy, conducting vulnerability assessments, security incident planning, and tools and practices for critical information asset protection.

The SANS/FBI Top Twenty Most Critical Internet Security Vulnerabilities

This is published by the SANS Institute. It is available at **http://www.sans.org/top20.htm**. The SANS/FBI Top Twenty is a list of critical Internet security vulnerabilities (e.g., default installs of operating systems and applications), how to determine if you are vulnerable, and how to protect against it.

It is anticipated that these requirements will be subject to audit in the near future. This listing and related subjects will be periodically updated and the process of identifying and implementing security controls should be viewed as an ongoing effort.

If you have any questions regarding this budget letter, please contact Patricia Kuhar, Finance, Technology Oversight and Security Unit, at (916) 445-7077.

/s/ KATHRYN RADTKEY-GAITHER

KATHRYN RADTKEY-GAITHER
Assistant Director, Operations

Attachment