BUDGET LETTER

NUMBER: 03-13	
SUBJECT: ASSESSMENT OF INFORMATION TECHNOLOGY SECURITY MEASURES, POLICIES, AND PRACTICES	**DATE ISSUED:** June 9, 2003
REFERENCES: MANAGEMENT MEMO 02-20, BUDGET LETTER 02-29, GOVERNMENT CODE SECTION 6255, STATE ADMINISTRATIVE MANUAL SECTION 4841.3, AND BUDGET LETTER 03-11	**SUPERSEDES:**

TO: Agency Secretaries
Agency Information Officers
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 to your Departmental Information Security Officers and Departmental Chief Information Officers even though the Office of the State Information Security Officer will also distribute it separately.

BACKGROUND

The Department of Finance (Finance) is responsible for information technology (IT) security policy and oversight. In light of ongoing national security threats and instances of computer hacking and computer crime, it is increasingly important that the State employ consistent and effective security practices in all departments. To identify whether the State has appropriate high-value risk reduction measures and practices in place, Finance is issuing a departmental self-assessment, which must be completed by all departments and returned to Finance. The assessment will be delivered to department Chief Information Officers (CIOs) and Information Security Officers (ISOs) separately. Due dates for the assessment response are listed on the second page of this Budget Letter.

The assessment's technical questions apply to all systems and computer equipment in your department, including networks, computer systems, internet applications, LANs, servers, and all other computer equipment and applications. In addition to your main facilities, you must also evaluate systems and equipment located in satellite offices, branches, district offices, field offices, laboratories, State hospitals, correctional facilities, and all other State facilities. You must include all of these in the response, even if they are not controlled by the department's CIO or IT staff.

The assessment has two parts. Part I contains technical information and questions, and these address industry standard security measures that should already be in place throughout the state.

Part II of the assessment addresses policy and practice. You will be asked whether your department is in compliance with State security policy, and about specific departmental policies. There is an additional section that does not require response, describing key practices that each department should have in place to be consistent with standard security industry practice. You will be surveyed again in the future about your department's status on policy and practice items.

All departments must completely address the technical issues in Part I of the assessment. If you are not fully compliant you must submit a compliance plan to describe how your department will accomplish this within three months of submission of the response. If you will not become compliant, you must explain how you are managing each of the stated problem areas in lieu of applying the required safeguards. The plans and/or non-compliance explanations must be approved by the department director, and must be submitted with the assessment response. You may use the space at the bottom of the assessment's cover sheet to provide the plans, or you may attach additional pages.

The security assessment is not comprehensive and does not attempt to cover all possible safeguards and security measures. We are targeting the assessment to cover actions and practices that can be implemented within existing resources, at little or no cost, and have a high pay-off value in terms of risk reduction. You will find that the measures and practices we ask about are consistent with what is recommended on well-known security industry web sites, such as www.sans.org. To identify and manage security risk involving other technologies or other topics, please refer to industry information that is readily available on the Internet, in printed reference material, or through professional security associations.

Management Memo 02-20 and Budget Letters 02-29 and 03-11 clarified Information Technology Policy, Instructions, and Guidelines, and required departments to verify that appropriate information security controls were in place. Departments were not required to submit reports to Finance of that validation. This current self-assessment includes questions about some of the same controls and this time responses are required. Previously, the Department of Information Technology conducted surveys and sent self-assessments to some departments. Some of the questions from those surveys are also included in this self-assessment, but may have been updated to reflect current vulnerabilities. In the constantly changing IT security area, it is important to periodically re-assess security measures and practices to ensure that State technologies are keeping up with known risks and vulnerabilities.

The State ISO Office will use this information to identify areas that need attention, help departments focus on high pay-off remedial actions, and identify needed follow-up activities. We will review each department's security assessment individually, and keep all information confidential. We will retain the information for future reference.

In selected cases, follow-up to the assessment responses may include scheduled on-site assessments from a team that will be assembled by Finance. The assessment team will validate responses, check for compliance, and identify outstanding security issues.

COMPLETION OF THE ASSESSMENT AND DELIVERY TO FINANCE

The due dates for the assessments are staggered, in four groups, and are based on department size. This is the schedule of due dates:

Departments with fewer than 100 State employees	June 30, 2003
Departments with 101-200 State employees	July 31, 2003
Departments with 201-1000 State employees	August 29, 2003
Departments with more than 1,000 State employees	September 30, 2003

All departments must file the report, on paper, with its attached cover sheet, signed by the department director, ISO, and CIO. Please mail or deliver the report to the Department of Finance, State ISO Office, 915 L Street, 6th Floor, Sacramento, CA 95814. Please mark your response package "Confidential."

CONFIDENTIALITY

The State ISO Office staff will maintain the confidentiality of your response, consistent with Government Code Section 6255. Also see the State Administrative Manual Section 4841.3, which allows us to handle material with the same degree of confidentiality as you do. If your department receives a follow-up on-site assessment, the assessment team will be bound by the same confidentiality requirements.

CONTACTS AND QUESTIONS

You may call the State ISO Office at 916-445-5239 if you have questions about the assessment. If your department did not receive a copy of the assessment form, please use this telephone number to advise us of correct contact information for your ISO and CIO.

/s/ KATHRYN RADTKEY-GAITHER

KATHRYN RADTKEY-GAITHER
Assistant Director