February 28, 2000

M-00-07

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM:
Jacob J. Lew
Director

SUBJECT:
Incorporating and Funding Security in Information Systems Investments

This memorandum reminds agencies of the Office of Management and Budget's (OMB) principles for incorporating and funding security as part of agency information technology systems and architectures and of the decision criteria that will be used to evaluate security for information systems investments. The principles and decision criteria are designed to highlight our existing policy and thereby foster improved compliance with existing security obligations; this memorandum does not constitute new security policy. OMB plans to use the principles as part of the FY 2002 budget process to determine whether an agency's information systems investments include adequate security plans.

Protecting the information and systems that the Federal government depends on is important as agencies increasingly rely on new technology. Agencies are working to preserve the integrity, reliability, availability, and confidentiality of important information while maintaining their information systems. The most effective way to protect information and systems is to incorporate security into the architecture of each. This approach ensures that security supports agency business operations, thus facilitating those operations, and that plans to fund and manage security are built into life-cycle budgets for information systems.

This memorandum is written pursuant to the Information Technology Management Reform Act (the Clinger-Cohen Act) which directs OMB to develop, as part of the budget process, a mechanism to analyze, track, and evaluate the risks and results of major capital investments made by an executive agency for information systems. Additionally, the Clinger-Cohen Act calls for OMB to issue clear and concise direction to ensure that the information security policies, processes, and practices of the agencies are adequate. These criteria will be incorporated into future revisions of OMB Circular A-130 ("Management of Federal Information Resources") and should be used in conjunction with previous OMB guidance on sound capital planning and investment control in OMB Memorandum 97-02, "Funding Information Systems Investments"; OMB Memorandum 97-16, "Information Technology Architectures"; and subsequent updates.

Security programs and controls implemented under this memorandum should be consistent with the Computer Security Act, the Paperwork Reduction Act, the Clinger-Cohen Act, and OMB Circular A-130. They should also be consistent with security guidance issued by the National Institute of Standards and Technology (NIST). Security controls for national security telecommunications and information systems should be implemented in accordance with appropriate national security directives.

Principles

The principles outlined below will support more effective agency implementation of both agency computer security and critical information infrastructure protection programs. In terms of Federal information systems, critical infrastructure protection starts with an effort to prioritize key systems (e.g., those that are most critical to agency operations). Once systems are prioritized, agencies apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of likely harm.

- Agencies should develop security programs and incorporate security and privacy into information systems with attention to the following principles:

- Effective security is an essential element of all information systems.

- Effective privacy protections are essential to all information systems, especially those that contain substantial amounts of personally identifiable information. The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal information.

- The increase in efficiency and effectiveness that flows from the use of interconnected computers and networks has been accompanied by increased risks and potential magnitude of loss. The protection of Federal computer resources must be commensurate with the risk of harm resulting from any misuse or unauthorized access to such systems and the information flowing through them.

- Security risks and incidents must be managed in a way that complements and does not unnecessarily impede agency business operations. By understanding risks and implementing an appropriate level of cost-effective controls, agencies can reduce risk and potential loss significantly.

- A strategy to manage security is essential. Such a strategy should be based on an ongoing cycle of risk management and should be developed in coordination with and implemented by agency program officials. It should identify significant risks, clearly establish responsibility for reducing them, and ensure that risk management remains effective over time.

- Agency program officials must understand the risk to systems under their control and determine the acceptable level of risk, ensure that adequate security is maintained to support and assist the programs under their control, and ensure that security controls comport with program needs and

appropriately accommodate operational necessities. In addition, program officials should work in conjunction with Chief Information Officers and other appropriate agency officials so that security measures support agency information architectures.

Policy

Security should be built into and funded as part of the system architecture. Agencies should make security's role explicit in information technology investments and capital programming. These actions are entirely consistent with and build upon the principles outlined in OMB Memorandum 97-02. Accordingly, investments in the development of new or the continued operation of existing information systems, both general support systems and major applications, proposed for funding in the President's budget must:

1. **Be tied to the agency's information architecture**. Proposals should demonstrate that the security controls for components, applications, and systems are consistent with and an integral part of the information technology architecture of the agency.

2. **Be well-planned, by**:

a) Demonstrating that the costs of security controls are understood and are explicitly incorporated in the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming.

b) Incorporating a security plan that discusses:

- the rules of behavior for the system and the consequences for violating those rules;
- personnel and technical controls for the system;
- methods for identifying, appropriately limiting, and controlling interconnections with other systems and specific ways such limits will be monitored and managed;
- procedures for the on-going training of individuals that are permitted access to the system;
- procedures for the on-going monitoring of the effectiveness of security controls;
- procedures for reporting and sharing with appropriate agency and government authorities indications of attempted and successful intrusions into agency systems;
- provisions for the continuity of support in the event of system disruption or failure.

3. **Manage risks, by**:

a) Demonstrating specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time.

b) Demonstrating specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages.

c) Identifying additional security controls that are necessary to minimize risks to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control.

4. **Protect privacy and confidentiality, by**:

a) Deploying effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access.

b) Ensuring that the handling of personal information is consistent with relevant government-wide and agency policies, such as privacy statements on the agency's web sites.

5. **Account for departures from NIST Guidance**. For non-national security applications, to ensure the use of risk-based cost-effective security controls, describe each occasion when employing standards and guidance that are more stringent than those promulgated by the National Institute for Standards and Technology.

In general, OMB will consider new or continued funding only for those system investments that satisfy these criteria and will consider funding information technology investments only upon demonstration that existing agency systems meet these criteria. Agencies should begin now to identify any existing systems that do not meet these decision criteria. They should then work with their OMB representatives to arrive at a reasonable process and timetable to bring such systems into compliance. Agencies should begin with externally accessible systems and those interconnected systems that are critical to agency operations. OMB staff are available to work with you if you or your staff have questions or need further assistance in meeting these requirements.