EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-06-19

July 12, 2006

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information[1] and to remind you of existing requirements, and explain new requirements your agency will need to provide addressing security and privacy in your fiscal year 2008 budget submissions for information technology (IT).

Reporting Security Incidents

As you know, the Federal Information Security Management Act of 2002 requires all agencies to report security incidents to a Federal incident response center. The center (US-CERT) is located within the Department of Homeland Security. The specific reporting procedures are found in the concept of operations for US-CERT. [2]

As you know, the reporting procedures require agencies to report according to various timeframes based on type of incident. This memorandum revises those reporting procedures to now require agencies to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident.[3] You should report all incidents involving personally identifiable information in electronic or physical form and should not distinguish between suspected and confirmed breaches. US-CERT will forward all agency reports to the appropriate Identity Theft Task Force point-of-contact also within one hour of notification by an agency.

Incorporating Security Funding Into Information Technology Investments

[1] For purposes of this policy, the term Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

[2] See US-CERT website at http://www.us-cert.gov/federal/reportingRequirements.html

[3] Loss of PII information on Department of Defense or Intelligence Community networks must also be reported by the individual agency CERTs to US-CERT within one hour.

On April 25, 2006, Clay Johnson sent to the heads of departments and agencies planning guidance for the President's fiscal year 2008 budget request.[4] In that context, I wanted to (1) remind you of the security and privacy requirements you should include within your IT investments and (2) explain additional items you will need to provide in your materials.

In particular, I want to remind you of Office of Management and Budget (OMB) Memorandum M-00-07, of February 28, 2000, "Incorporating and Funding Security in Information Systems Investments," instructs agencies on how to include security into the funding for information technology.[5] This guidance is also included in OMB's budget preparation policy, i.e., Circular A-11 and requires you to do two specific things. Under these existing guidance requirements, first, you must integrate security into and fund it over the lifecycle of each system undergoing development, modernization, or enhancement. Second, your steady-state system operations must meet existing security requirements before new funds are spent on system development, modernization or enhancement.

In addition, please provide additional detail on how you are allocating your resources between correcting existing security weaknesses in stead-state investments and proposing funds for system development, modernization, or enhancement.

Finally, for those agencies having significant isolated or wide-spread weaknesses identified by the agency Inspector General or the Government Accountability Office, please identify the specific funds you are requesting for proposed development, modernization, or enhancement efforts to correct these security weaknesses. This includes correcting weaknesses found during your privacy program reviews required by OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information"[6] and for implementing the specific security controls set forth in OMB Memorandum M-06-16, "Protection of Sensitive Agency Information."[7]

---

[4] See OMB's website at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-14.pdf
[5] See OMB's website at http://www.whitehouse.gov/omb/memoranda/m00-07.html
[6] See OMB's website at http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf
[7] See OMB's website at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf