



United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240



Memorandum

DEC 15 2006

To: Heads of Bureaus and Offices
Bureau and Office Chief Information Officers

From: W. Hord Tipton 
Chief Information Officer

Subject: Additional Guidance for the Protection of Personally Identifiable Information (PII) and Department Sensitive Information

This memorandum provides additional guidance regarding requirements previously specified in the "Protection of Personally Identifiable Information (PII) and Department Sensitive Information" memorandum issued on September 8, 2006.

1. Per the September 8, 2006 memorandum, bureaus and offices were required to ensure FIPS 140-2 validated encryption of all mobile media and devices (e.g., removable media, portable/mobile devices, remote workstations, etc.) containing agency data taken outside of the Agency's secured physical perimeter (e.g., to a personal residence, on either business or personal travel – even if traveling to another controlled facility, etc.). unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual designated in writing by the Deputy Secretary.

Additional Guidance: As an interim mitigation to the risks associated with the potential loss or theft of PII or Department sensitive information, bureaus and offices that currently do not have an encryption solution for mobile devices (e.g., laptops and remote workstations/servers) are minimally required to take the following actions until an Enterprise-wide encryption solution can be procured.

Within 60 days from issuance of this memorandum:

- implement the Encrypting File System (EFS), or equivalent, for Windows-based systems;
- implement FileVault, or equivalent, for Macintosh-based systems; and
- for other operating systems, bureaus and offices must identify and implement an appropriate solution to provide file-level encryption at a minimum.

2. A standard secondary Message Banner for deployment on all remote access points was developed by the Encryption Working Group (EWG) and has been approved by the Solicitor's Office. The previous memorandum requires deployment of the following Message Banner within five days of issuance of this memorandum:

WARNING - Before you download Department of the Interior (DOI) data to a computer or any other device capable of storing electronic data you must comply with DOI standards for data encryption and system security. You must also understand and agree to comply with DOI requirements for deleting the data. Contact your IT Security Manager for specifications regarding these standards and requirements. Failure to comply may result in criminal, civil, and/or disciplinary action.

3. Bureaus and offices were are required to have equivalent language to the following standard elements, or incorporate those elements into their existing Rules of Behavior (RoB), to address the protection of PII and sensitive data, Remote Access, and mobile computing device usage. The Solicitor's Office has approved the following standard RoB elements developed by the EWG after a thorough review by the Human Resources Office and a representative subset of government worker Unions:

Special Considerations for Remote Access - Access of agency resources from a location not under the direct control of the ESN or {bureau or office name} is considered "Remote Access". New technical solutions are being implemented to secure and protect agency data, especially if it is being carried outside of the ESN or {bureau or office name}'s physically protected areas. With these new requirements also come new responsibilities for user behavior regarding the protection of agency data. Users must secure and protect agency data as follows:

- *Users must physically protect all hardware or software based tokens entrusted to them for authentication or encryption purposes. (A token is usually a physical device that an authorized user is given to provide additional higher level security and to verify the user is who they say they are when logging in to the network.)*
- *Users must encrypt all agency data stored on any equipment, including but not limited to computers, external hard drives, PDAs, and thumb/flash drives, anytime they are outside of {bureau or office name} protected facilities.*
- *Users must ensure that all agency data downloaded using remote access is erased after 90 days or when it is no longer needed.*
- *Users should refer to their IT Security Manager for standards and approved methods for encrypting and deleting data.*

4. Bureaus and offices not having implemented the requirements specified in the previous memorandum by September 30, 2006 were to develop, maintain, and revise as necessary Plans of Action and Milestones (POA&Ms). To assist bureaus and offices, the Department's Cyber Security Division (CSD) developed standard POA&M elements to be included in the Department's POA&M, as well as POA&M template elements to be incorporated by each bureau and office in their respective Program- or system-level POA&Ms as each bureau deems most appropriate. Those standard POA&M template elements are attached.
5. OMB memorandum M-06-16 requires determinations of non-sensitive data to be in writing by the Deputy Secretary, or an individual designated in writing by the Deputy Secretary, in order to waive the encryption requirements on specific mobile devices. On August 3, 2006, the Deputy Secretary delegated this authority to the Department CIO and restricted further delegation of this authority. To enable the CIO to accurately evaluate requests for determination of non-sensitive data in a system, the attached "Certification and Request for Determination of Non-Sensitive Data" request template shall be used. The signature of the Designated Approving Authority (DAA) on the request shall be the senior management official, within the requesting bureau or office, designated as the DAA responsible for risk acceptance and accreditation of the Certification and Accreditation (C&A) information system boundary with which the mobile computing devices are associated.

Attachments

cc: Bureau and Office Deputy Chief Information Officers
Bureau IT Security Managers