USDA

United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

JUL 13 2006

TO: Agency Chief Information Officers
Agency Information System Security Program Managers

FROM: Lynn Allen
Associate Chief Information Officer
Cyber Security

SUBJECT: Interim Steps for Office of Management and Budget (OMB) Memorandum 06-16

On June 23, 2006, OMB issued guidance that requires federal agencies to take four specific actions to protect Privacy Act and other sensitive data on agency systems within 45 days. OCIO established a working group, chaired by my Operations group, to address the first two requirements: (1) encryption of portable devices and (2) use of two-factor authentication. The working group will identify processes, evaluate products, and establish a timeline to implement the OMB mandate successfully Department-wide.

In the interim, individual agencies can take several actions, which have little to no cost associated with them, to protect our sensitive information. While these actions are not long-term solutions, they are 'first steps' in protecting your data. Agencies are encouraged to implement those that you feel work best in your environment.

1. <u>Encrypt all data on mobile devices/computers</u>

   - Inform users what data is considered sensitive within your agency and remind them of their responsibilities for protecting such data.
   - Use the Encrypted File System (EFS) available in current versions of Microsoft Windows
   - Use the built-in encryption function in Microsoft Excel or Word, or use inexpensive encryption software in compression software (i.e., WinZip) or similar programs.
   - Replace existing USB 'thumb' drives with ones that are accompanied by strong encryption software.
   - When obtaining data extracts from databases, do not include Privacy Act protected or other sensitive data unless absolutely necessary.
   - Ensure that contracts explicitly require that contractors are responsible for controlling and protecting Privacy Act and other sensitive data in their possession, and that they destroy such data when the contract has ended.

2. Remote Access with two-factor authentication

- Do not allow traffic from remote access software through your firewall. Instead, require telework employees and contractors to enter the network through a Virtual Private Network (VPN), before launching remote access software.
- Limit remote access through VPN by specific Internet Protocol (IP), or hardware (MAC) address rather than allowing anyone to make such a connection.
- Remind employees to use strong passwords, and enforce the use of such strong passwords within the operating system when possible. Strong passwords are at least eight characters long and include a combination of upper and lower-case letters, numbers, and special characters.
- Ensure that default software passwords are changed to strong passwords as defined above.
- Rename the Administrator account in Windows and ensure that Guest accounts are disabled.

The third and forth actions outlined in the OMB memorandum are security practices that should already be in place. Please review your policies and processes to ensure that controls have been established and are operating effectively for these two items.

The full text of OMB's memorandum can be found on OMB's website www.whitehouse.gov/omb. If you have any questions, please contact Steven Bryce Eckland, Computer Security Operations Division, at 816-926-7330.

cc:
Dave Combs, Chief Information Officer
Jerry Williams, Deputy Chief Information Officer