



JUN 27 2006

United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

MEMORANDUM FOR USDA AGENCY CIOs

FROM: Dave Combs
USDA Chief Information Officer

SUBJECT: Review of Lost or Stolen Items containing Sensitive Information

With this memorandum, I am requiring an immediate review of all lost or stolen items containing sensitive information to be submitted to the USDA Office of Cyber Security (cyber.security@usda.gov) no later than July 31, 2006. This would include personal computers (desktops and laptops), personal digital assistants (PDAs), removable media (i.e., floppy diskette, thumb drives, etc.) and all other devices that could contain sensitive information. For the purposes of this review, the National Institute of Standards and Technology's (NIST) definition will prevail. NIST defines "sensitive" information as any information, for which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

The overall objective of this limited scope review is to assess the sufficiency of USDA's systems and procedures in providing select management information concerning missing computers and other sensitive items of inventory, and possible disclosure of sensitive information for the last three years, beginning January 1, 2003 to date. Agencies should take steps to assess the sufficiency of existing inventory controls, including documentation that would fully support disposition of missing items and, inventory systems containing sensitive information and ensure that such information is encrypted in a manner that would eliminate unauthorized disclosure as outlined in OMB Memorandum M-06-16.

Any missing/stolen computer equipment/media with storage capacity containing sensitive information identified during this review and in the future should be treated as a Cyber Security incident and reported immediately to Cyber Security in accordance with Department Manual (DM) 3505-000, dated March 20, 2006. Agencies should take immediate action to determine if any information on these devices has an impact to the public, customers, agency mission, or the Department, and take the appropriate actions as necessary.

USDA's Cyber Security Office, the main point of contact for US-Cert, will report any such incident according to its reporting guidelines and follow up

with agency personnel until the incident is closed. Agencies should not report directly to US-Cert.

Please contact Mary Heard at (202) 720-0492 if you have questions.