MEMORANDUM FOR CHIEF INFORMATION OFFICERS

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

SUBJECT: Top 10 Risks Impeding the Adequate Protection of Government Information

In order to maintain the trust of the American public, we must operate effectively by securing government information and safeguarding personally identifiable information in our possession. To make the federal government's identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the President's Identity Theft Task Force recently issued "Combating Identity Theft: A Strategic Plan."

The strategic plan instructed the Office of Management and Budget and the Department of Homeland Security to develop the attached paper identifying common risks (or "mistakes") and best practices to help improve your agency's security and privacy programs. Each risk is associated with selected best practices and important resources to help your agency mitigate and avoid these risks. All of the best practices and important resources are inter-related and complementary, and they can be broadly applied when administering your information security and privacy programs.

Common Risks Impeding the Adequate Protection of Government Information

Sponsored by

The Department of Homeland Security and the Office of Management and Budget

As Directed by

The Identity Theft Task Force

July 2007

Introduction

To ensure government agencies receive specific guidance on concrete steps they can take to improve their information security measures, the President's Identity Theft Task Force recommended the Office of Management Budget (OMB) and the Department of Homeland Security (DHS):

- outline best practices in the area of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs; and
- develop a list of the most common 10 or 20 "mistakes" to avoid in protecting information held by the government.[1]

This paper identifies common risks, or "mistakes," impeding agencies from adequately protecting government information. Each risk is associated with selected best practices and important resources to help agencies mitigate and avoid these risks; best practices and important resources are inter-related and complementary. Agencies may refer to this paper when considering steps necessary for administering agency information security and privacy programs as required by law, policy, and guidance.

The paper incorporates comments received during a public forum hosted on May 11, 2007 by DHS and OMB, as well as comments received through interagency review. Other resources were incorporated in developing this paper, including the DHS interagency Critical Infrastructure Protection Cyber Policy Coordinating Committee Working Group's whitepaper titled "Network Architecture and Data Handling."

Common Risks Impeding the Adequate Protection of Government Information

1. Security and privacy training is inadequate and poorly aligned with the different roles and responsibilities of various personnel.

Best Practices

- Agencies identify personnel with significant security and privacy responsibilities, and tailor training to support various roles and responsibilities commensurate with respective responsibilities.
- Agencies provide security and privacy training for all personnel upon hiring and at least annually. Both initial and refresher training explain acceptable rules of behavior and the consequences when rules are not followed.
- Agencies assess whether training is effective, and adapt training to address changing requirements and emerging threats.
- Agencies require personnel to sign documentation verifying they completed training, track the number of personnel trained, and consider whether training was completed when evaluating personnel performance.
- Agencies use creative methods to promote daily awareness of employees' privacy and security responsibilities, such as providing weekly tips, annual "security days," FAQs,

[1] The Identify Theft Task Force Strategic Plan can be found at: http://www.idtheft.gov/reports/StrategicPlan.pdf.

mouse pads imprinted with security reminders, privacy screens when using laptops in public, and incentives for reporting security risks.

Important Resources

- The National Institute of Standards and Technology (NIST) Special Publications 800-50, "Building an Information Technology and Security Awareness Training Program" and 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," at: http://csrc.nist.gov/publications/nistpubs/index.html.
- Shared Service Centers participating in the Information Systems Security Line of Business provide agencies a baseline level of security awareness training. To learn more see: http://www.whitehouse.gov/omb/egov/c-6-6-its.html.

2. Contracts and data sharing agreements between agencies and entities operating on behalf of the agency do not describe the procedures for appropriately processing and adequately safeguarding information.

Best Practices

- Agencies establish contracts and agreements describing the procedures for appropriately using and adequately protecting information, and identify who is responsible for ensuring the procedures are completed.
- Agencies incorporate standardized Federal Acquisition Regulation (FAR) language when developing contracts and agreements.
- Agency contracts and agreements include incentives and awards for successfully completing the procedures described for appropriately using and adequately protecting information.

Important Resources

- NIST Special Publications 800-53, "Recommended Security Controls for Federal Information Systems," 800-37, "Guide for Security Certification and Accreditation of Federal Information Systems," and 800-47, "Security Guide for Interconnecting Information Technology Systems," at: http://csrc.nist.gov/publications/nistpubs/index.html.
- The Federal Acquisition Regulation, Subpart 7.1—Acquisition Plans, requires heads of agencies to ensure agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology.

3. Information inventories inaccurately describe the types and uses of government information, and the locations where it is stored, processed or transmitted, including personally identifiable information.

Best Practices

- Agencies use their enterprise architectures and inventories of information collections to maintain an understanding of the types and uses of information collected and processed at their agency, and to ensure information is used to support the proper performance of agency function.
- Agencies regularly review the types of information collected, created, maintained, extracted, disposed, and archived (i.e., processed) by their agency to verify whether information is required for the proper performance of an agency function or needed for a documented legal or business need.
- Agencies use their inventory when determining which security controls are necessary to adequately secure information.
- Agencies regularly review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

Important Resources

- The Paperwork Reduction Act requires agencies to manage information collections from the public in the manner prescribed in OMB's guidance in 5 CFR section 1320. For additional information see: http://www.access.gpo.gov/nara/cfr/waisidx_99/5cfr1320_99.html.
- An enterprise architecture is an explicit description and documentation of the current and desired relationships among business and management processes and information technology. In the creation of an enterprise architecture, agencies must define the data and describe the relationships among data elements used in the agency's information systems at a high level. For more information see: http://www.whitehouse.gov/omb/egov/a-1-fea.html.
- NIST Special Publications 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories," and 800-53, "Recommended Security Controls for Federal Information Systems," at: http://csrc.nist.gov/publications/nistpubs/index.html.
- OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," located at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf, and OMB Circular A-130, "Management of Federal Information Resources," at: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

4. Information is not appropriately scheduled, archived, or destroyed.

Best Practices

- Agencies obtain NARA's approval for the disposition of their information holdings by establishing records schedules, as required by 44 U.S.C. 3303.
- Agencies use these records schedules to determine how long information needs to be maintained, and whether it needs to be archived (i.e., transferred to NARA) or can be destroyed.

Important Resources

- The National Archives and Records Administration provides agencies records management regulations (36 CFR, part 1228) and guidance; for more information see: http://www.archives.gov/records_management/index.html.
- NIST Special Publication 800-88, "Guidelines for Media Sanitization," at: http://csrc.nist.gov/publications/nistpubs/index.html.

5. Suspicious activities and incidents are not identified and reported in a timely manner.

Best Practices

- Agencies develop and implement standard operating procedures describing how to identify and report suspicious activities and incidents.
- Agencies report suspicious activities and incidents in a timely manner to mitigate harm and prevent similar incidents from re-occurring.
- Agencies configure systems to log security events and monitor the logs to detect suspicious activity.
- Agency information security personnel who administer the agency's incident handling activities collaborate closely with agency program officers and are enrolled with the Government Forum of Incident Response and Security Teams (GFIRST).
- Agencies use enterprise applications to detect intrusions, and correlate and prioritize responses to security incidents across the agency.
- Agencies document lessons learned after responding to incidents and incorporate them into security and privacy awareness training accordingly.
- Agencies route employee web traffic through approved servers to simplify the monitoring of web traffic for malicious content.
- Agencies report incidents concerning personally identifiable information to United States – Computer Emergency Readiness Team (US-CERT) within one hour, and use their breach notification policy and plan, as necessary.
- Agencies utilize anti-spam filtering solutions to reduce suspicious emails (e.g., spam, phishing, social engineering) received by users.

Important Resources

- Agency procedures for handling incidents can be found at US-CERT's Concept of Operations at: http://www.us-cert.gov/federal/reportingRequirements.html.
- NIST Publications 800-61, "Computer Security Incident Handling Guide," at: http://csrc.nist.gov/publications/nistpubs/index.html.

- Agencies can participate in GFIRST and the US-CERT's Einstein program, an automated process for collecting, correlating, analyzing, and sharing of computer security information across the Federal civilian government.
- OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

6. Audit trails documenting how information is processed are not appropriately created or reviewed.

Best Practices

- Agencies move information into a managed data repository to develop and review audit trails, and verify whether the use of the information is consistent with any applicable NARA-approved records retention and disposition schedules.
- Agencies log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.
- Agencies use information provided by audit trails to identify anomalies in accessing information and determine whether information is no longer needed for the proper performance of agency function.

Important Resources

- OMB Memorandums M-06-16, "Protection of Sensitive Agency Information," and M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," at: http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf, and http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf, respectively.
- NIST Publication 800-92, "Guide to Computer Security Log Management," and NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," found at: http://csrc.nist.gov/publications/nistpubs/index.html.

7. Inadequate physical security controls where information is collected, created, processed or maintained.

Best Practices

- Agencies maintain an accurate inventory of their property (e.g., retail, industrial, commercial, agricultural and other types of real estate).
- Agencies maintain an accurate inventory of their portable and mobile devices.
- Agencies locate where high-impact and high-risk information systems operate, and apply commensurate controls to mitigate risk.
- Agencies regularly review procedures, at least annually, for allowing physical access to buildings and specific areas to only those who are authorized.

Important Resources

- Executive Order 13327, "Federal Real Property Asset Management," provides policy for effective real property asset management. For more information, see: http://www.whitehouse.gov/news/releases/2004/02/20040204-1.html.
- Homeland Security Presidential Directive 12 provides policy for a common identification standard for Federal employees and contractors. For more information see: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html, OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors," at: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf, and NIST Federal Information Processing Standard (FIPS) 201, "Personal Identity Verification of Federal Employees and Contractors," at: http://csrc.nist.gov/publications/fips/index.html.
- NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," found at: http://csrc.nist.gov/publications/nistpubs/index.html.

8. Information security controls are not adequate.

Best Practices

- Security controls are tested regularly, and at least annually, to ensure they are effective.
- Personnel who test controls work closely with, but remain separate from, the personnel administering them.
- Agencies share the results from control testing quickly with those who need to improve them.
- Agencies reduce security costs by centrally managing the development, implementation, and assessment of the common security controls designated by the agency—and subsequently, share assessment results with the owners of information systems where those common security controls are applied.
- Agencies adopt common security configurations maintained by NIST, deploy tested patches quickly, and use the security content automation protocol methodology to enable automated vulnerability management, measurement, and policy compliance evaluation.
- Agencies maintain an accurate plan of action and milestones to fix security controls needing improvement.
- Agencies consider the public availability of related information as a factor when determining how to protect government information.

Important Resources

- The Security Content Automation Program (SCAP) enables organizations to automate security compliance, manage vulnerabilities, and perform security measurement. For more information see: http://nvd.nist.gov/scap.cfm.
- OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," instructed senior agency officials for privacy to conduct a review of policy and processes.
- The Federal Trade Commission published a guidebook outlining steps for safeguarding information at: http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf.

- NIST operates the Program Review for Information Security Management Assistance to provide an independent review of the maturity of an agency's information security program. For more information, see: http://prisma.nist.gov/index.html.
- NIST Special Publications 800-53, "Recommended Security Controls for Federal Information Systems," 800-37, "Guide for Security Certification and Accreditation of Federal Information Systems," 800-40, "Creating a Patch and Vulnerability Management Program," and 800-94, "Guide to Intrusion Detection and Prevention Systems," at: http://csrc.nist.gov/publications/nistpubs/index.html.
- There are now over 120 common security configurations published on NIST's web site, for more information see: http://checklists.nist.gov.
- OMB Memorandums M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," and M-07-18 "Ensuring New Acquisitions Include Common Security Configurations," found at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf, and http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf, respectively, as well as OMB memorandum "Managing Security Risk By Using Common Security Configurations," at: http://www.cio.gov/documents/Windows_Common_Security_Configurations.doc.

9. Inadequate protection of information accessed or processed remotely.

Best Practices

- Agencies maintain an audit log of information accessed or processed remotely, as appropriate.
- Agencies use privacy screens when working outside the office and require employees to store laptop computers in carry-on luggage rather than checked baggage.
- Agencies encrypt, using only NIST certified cryptographic modules, remote access communications involving sensitive data and all sensitive data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by the agency's Deputy Secretary or a senior-level individual he/she may designate in writing.
- Agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
- Agencies use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity.
- Agencies develop and implement telework policies describing procedures personnel must take to securely access government information remotely.
- Agencies ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities, the rules of behavior associated with access to personally identifiable information, and the consequences for the loss and/or misuse of personally identifiable information.

Important Resources

- NIST Special Publications 800-53, "Recommended Security Controls for Federal Information Systems," 800-37, "Guide for Security Certification and Accreditation of

Federal Information Systems," and NIST FIPS 140-2, "Security Requirements for Cryptographic Modules," at: http://csrc.nist.gov/publications/nistpubs/index.html.

- OMB Memorandums M-06-16, "Protection of Sensitive Agency Information," and M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," located at: http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf, and http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf, respectively.

10. Agencies acquire information technology and information security products without incorporating appropriate security and privacy standards and guidelines.

Best Practices

- Agencies incorporate the costs for security and privacy in their information technology investments and throughout the system development life-cycle, including information system planning, development and maintenance.
- Agencies demonstrate the costs of security and privacy controls are understood and are explicitly incorporated in the life-cycle planning of the overall system in a manner consistent with agency capital planning and investment control procedures.
- Agencies consider new or continued funding only for those system investments demonstrating procedures necessary for adequately securing information are completed.
- Agencies acquire information technology products incorporating information security and privacy requirements, as appropriate.
- Agencies acquire software and hardware encryption products, and other security products, available under blanket purchase agreements competed using the General Services Administration's (GSA) government-wide SmartBUY program.
- Agencies implement a cryptographic key management program using NIST certified cryptographic modules.
- Agencies implement enterprise rights management and encryption technologies for Federal records in accordance with NARA guidance.

Important Resources

- NIST FIPS 140-2, "Security Requirements for Cryptographic Modules," and NIST FIPS 201, "Personal Identity Verification of Federal Employees and Contractors," at: http://csrc.nist.gov/publications/fips/index.html.
- NARA Bulletin 2007-2 provides guidance concerning the use of enterprise rights management and other encryption-related software on Federal records at: http://www.archives.gov/records-mgmt/bulletins/2007/2007-02.html.
- GSA's SmartBUY program supports cost-effective enterprise level software management through the aggregate buying of commercial software governmentwide, for more information see: http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8199&channelId=-18846.
- OMB Circular A-11, "Preparation, Submission and Execution of the Budget," (section 53 and 300, in particular), and OMB memorandums M-00-07 "Incorporating and Funding Security in Information Systems Investments," and M-06-17 "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in

Agency Information Technology Investments," found at:
http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html,
http://www.whitehouse.gov/omb/memoranda/m00-07.html, and
http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf, respectively.