Office of Management and Budget

FY 2006 Report to Congress on Implementation of The Federal Information Security Management Act of 2002

TABLE OF CONTENTS

I. Introduction

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). The goals of FISMA include development of a comprehensive framework to protect the government's information, operations, and assets. Providing adequate security for the Federal government's investment in information technology (IT) is a significant undertaking. In fiscal year 2006, the Federal agencies spent $5.5 billion securing the government's total IT investment of approximately $63 billion equating to approximately 9 percent of the total IT portfolio. As described in Chapter III, these funds were used for a variety of security programs including certification and accreditation of systems, testing of controls, and user awareness training.

FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen IT system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with FISMA.

To ensure the safeguard of personally identifiable information (PII), agencies are also required to report on several performance metrics related to information privacy. In addition to tracking the metrics required by the E-Government Act, agencies are also required to report on several additional metrics, including those required by the Privacy Act (5 U.S.C. § 552a), which OMB is charged with implementing.

This report informs Congress and the public of the Federal government's security performance, and fulfills OMB's requirement under FISMA to submit an annual report to the Congress. It provides OMB's assessment of government-wide IT security strengths and weaknesses and a plan of action to improve performance. It also examines agency status against key security and privacy performance measures from fiscal year 2002 through fiscal year 2006.

Data used within this report is based on fiscal year 2006 agency, IG, and privacy reports to OMB. Appendix A contains statistical summaries of security performance at 25 large agencies. Appendix B provides a summary of small and independent agency compliance with FISMA. Appendix C of the report summarizes the roles and responsibilities within the Federal government's IT security program.

II. OMB Security and Privacy Reporting Guidance

To acquire information needed to oversee agency security programs and develop this report, each year OMB issues reporting guidance to the agencies.[1] As in the past, this year's guidance included quantitative performance measures for the major provisions of FISMA to help identify agency status and progress. Many of this year's security performance measures are identical to past years' guidance. Consequently, areas of improvement, as well as areas requiring additional management attention are easily discernable.

OMB's guidance includes specific questions about individual FISMA requirements, including:

- developing and maintaining an inventory of major information systems (including national security systems) operated by or under the control of the agency, as originally required by the Paperwork Reduction Act of 1995 (44 U.S.C. §101 note). The inventory must be used to support monitoring, testing and evaluation of information security controls.

- providing information security for the information and information systems *that support the operations and assets of the agency*, including those provided or managed by another agency, contractor, or other source on behalf of the agency. Agencies using external providers must determine the risk to the agency is at an acceptable level.

- determining minimally acceptable system configuration requirements and ensuring compliance with them. In addition, agencies must explain the degree to which they implement and enforce security configurations.

- developing a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.[2]

Additionally, this year's guidance requested performance measures to assess the privacy of agencies' personal information. These performance measures reflect requirements from the E-Government Act, the Privacy Act, and related OMB memoranda.[3] OMB also requested agencies provide a copy of the results of the review conducted by its Senior Official

[1] See OMB Memorandum M-06-20 of July 17, 2006, "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," at www.whitehouse.gov/omb/memoranda/2006.html
[2] In OMB's FISMA guidance, this process is called a security plan of action and milestones (POA&M). POA&Ms are the authoritative management tool used by the agency (including the IG) to detail specific program and system-level security weaknesses, remediation needs, the resources required to implement the plan, and scheduled completion dates.

for Privacy pursuant to OMB memorandum 06-15, "Safeguarding Personally Identifiable Information."

III. Government-wide Findings

A. Progress in Meeting Key Security Performance Measures

The fiscal year 2006 agency FISMA reports reveal modest improvement and progress in meeting several key security performance measures:

- Certifying and accrediting systems. The number of certified and accredited systems rose from 85 percent to 88 percent. At the same time, agencies reported a 3 percent increase in the total number of IT systems – from 10,289 in fiscal year 2005 to 10,595 in fiscal year 2006. Several agencies made significant progress in fiscal year 2006, most notably the Department of Homeland Security (DHS) and the Department of State (DOS) for improved rates of certifications and accreditations. Thirteen agencies now report a certification and accreditation rate of 100 percent of operational systems.

- Testing of security controls and contingency plans. FISMA and OMB policy requires agencies to test system security controls annually. In fiscal year 2006, agencies tested security controls for 88 percent of systems and contingency plans for 77 percent of all systems, up from 61 percent and 72 percent respectively in fiscal year 2005. The Department of Defense (DOD) alone increased system testing by more than 30 percent from 2005 to 2006. Though rates of testing for system security controls and contingency plans increased, that improvement is largely attributable to moderate and low risk systems, as well as uncategorized systems. The percentage of uncategorized systems with tested security controls climbed from 42 percent to 93 percent. OMB continues to track this metric quarterly, by risk impact level, and uses this metric as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Assigning a risk impact level.[4] Agencies reported a total of 10,595 systems categorized by a risk impact level of high, moderate, low, or undetermined. Of these, 9,388 systems

[3] Related memoranda include M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Circular A-130, Appendix I "Federal Agency Responsibilities for Maintaining Records About Individuals."

[4] In February 2004, NIST issued Federal Information Processing Standard 199 "Standards for Security Categorization of Federal Information and Information Systems". The standard establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and

were managed by Federal agencies and 1,207 were managed by a contractor or other organization on behalf of a Federal agency. Overall, 1,367 agency systems were categorized as high impact, 3,174 as moderate impact, and 4,516 as low impact. Of the 1,207 contractor systems, 236 were categorized as high impact, 397 as medium impact, and 205 as low impact. As of October 2006, agencies reported that 331 agency systems and 369 contractor systems had not yet been assigned a risk impact level, representing almost 7 percent of the overall system inventory. The overall certification and accreditation percentage for high impact systems increased from 88 percent to 89 percent, which is still higher than the overall certification and accreditation average; however, uncategorized systems had the highest certification and accreditation average at 92 percent, an increase of 35 percent from 2005. Four agencies have a significant number of uncategorized systems, and two of those four have higher certification and accreditation rates for uncategorized systems than high, moderate or low risk systems. This suggests these agencies are not prioritizing their systems and working to secure the systems presenting the highest risk impact level, nor do they know at what level to secure those systems not categorized. OMB intends to follow up individually with these agencies.

- Employee training in systems security. Agencies reported increases in the percentage of employees receiving security awareness training and for employees with significant information security responsibilities, up 10 percent and 3 percent respectively from the prior year.

- Incident reporting. Agencies reported more than a 75 percent increase in the number of incidents reported internally and to US-CERT[5] from 2005, however, while incidents reported to law enforcement decreased dramatically from nearly 7,000 in 2005 to 900 in 2006.

---

threat information in assessing the risk to an organization. The process used by agencies to determine FIPS 199 categories is similar to the December 2003 Homeland Security Presidential Directive (HSPD) -7 requirement to identify, prioritize and protect critical infrastructure. Those cyber assets identified as "nationally critical" under HSPD-7 would be categorized as high impact under FIPS 199.

[5] DHS' incident response center (i.e., US-CERT) was created in September 2003. It provides timely technical assistance to agencies regarding security threats and vulnerabilities and compiles and analyzes information about security incidents. Additional information is provided in Appendix C of this report.

Below is a summary table (Table 1) showing progress in meeting selected government-wide goals:

Table 1: Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2006[6]					
Percentage of Systems with a:	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**
Certification and Accreditation	47%	62%	77%	85%	88%
Tested Contingency Plan	35%	48%	57%	61%	88%
Tested Security Controls	60%	64%	76%	72%	77%

While improvements have been made in fiscal year 2006, agency reports reveal areas requiring strategic and continued management attention over the coming year, including:

- Quality of certification and accreditation. IGs reported the overall quality of the certification and accreditation (C&A) processes at agencies decreased from 17 to 16 of the 25 agencies having a process in place rated as "satisfactory" or better. Eight agencies had C&A processes rated as "good" or "excellent," an increase from 5 in fiscal year 2005. Nine IGs reported overall C&A processes as "poor" or "failing," an increase of 1 from fiscal year 2005. This is an overall decrease in IG ratings from 2005, where 17 agencies were reported as "satisfactory" or better, yet the number of agencies moving to the "good" and "excellent" categories increased in 2006. OMB encourages agency CIOs and IGs to work together to improve the quality of the agency's C&A process, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Inventory of systems. IGs reported a slight decrease in the number of agencies with a system inventory over 80 percent complete, from 21 in 2005 to 20 in 2006. Though the majority of agency IGs reported inventories to be 96-100 percent complete, some agencies are still demonstrating large fluctuations in the number of systems in their inventories, both upwards and downwards.

[6] Total number of systems reported: fiscal year 2002=7957; fiscal year 2003=7998; fiscal year 2004=8623; fiscal year 2005=10289; fiscal year 2006=10595. The system count changes as agencies refine their system inventory and acquire, consolidate, or retire systems.
Total number of systems with a certification and accreditation: fiscal year 2002=3772; fiscal year 2003=4969; fiscal year 2004=6607; fiscal year 2005=8735; fiscal year 2006=9313
Total number of systems with a tested contingency plan: fiscal year 2002=2768; fiscal year 2003=3835; fiscal year 2004=4886; fiscal year 2005=6230; fiscal year 2006=9312
Total number of systems with tested security controls: fiscal year 2002=4751; fiscal year 2003=5143; fiscal year 2004=6515; fiscal year 2005=7425; fiscal year 2006=8144

- Oversight of contractor systems. OMB asked IGs to confirm whether the agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines. The majority (18 of 24) of agency IGs categorized the extent of agency's oversight as "frequently" (2 agencies), "mostly" (1 agency), and "almost always" (15 agencies); however, several (6 of 24) agency IGs rate the extent of agency oversight as "rarely" (3 agencies) or "sometimes" (3 agencies). These results remained the same as the prior reporting period. OMB encourages agency CIOs and IGs to work together to improve the quality of the agency's C&A process, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Agency-wide plans of action and milestones (POA&Ms). OMB policy requires agencies to prepare POA&Ms for all programs and systems where a security weakness has been found, and asks agency IGs to evaluate this process. Based on OMB analysis of IG reports, 19 agencies have effective POA&M processes; however reports from 6 other agencies reveal weaknesses which indicate ineffective processes. These numbers are the same as the numbers of effective POA&M processes reported in 2005, indicating no overall progress; however agencies that are rated as having effective processes are more often rated as being "almost always" effective rather than "mostly" effective. OMB encourages CIOs and IGs to work together to remediate these process weaknesses, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

In addition to the government-wide statistics above, Appendix A provides detail on individual Federal agencies' performance against key security and privacy performance measures. The tables within the appendix contain information from the agencies' fiscal year 2006 FISMA reports.

B. Progress in Meeting Key Privacy Performance Measures

The fiscal year 2006 agency FISMA reports reveal modest success in meeting several key privacy performance measures:

- Program Oversight. In 2006, the majority of agencies report having appropriate oversight of their privacy programs in place. All agencies report having a privacy official who participates in privacy compliance activities, although 84 percent report coordinated oversight coordination with their IG. Most agencies report privacy training for Federal employees and contractors, with 92 percent reporting general privacy training and 84 percent reporting job-specific privacy training.

- Privacy Impact Assessments. The Federal goal[7] is for 90 percent of applicable systems to have publicly posted privacy impact assessments (PIAs). In 2006, 84 percent of applicable systems government-wide have publicly posted privacy impact assessments. Although, 88 percent have written processes or policies for all listed aspects of PIAs.

- System of Records Notices. The Federal goal[8] is for 90 percent of applicable systems with PII contained in a system of records covered by the Privacy Act to have developed, published, and maintained systems of records notices (SORNs). In 2006, 83 percent of systems government-wide with PII contained in a system of records covered by the Privacy Act have developed, published, and maintained current SORNs.

IV. Government-wide IG Security Evaluation Results

Input from the agency IGs is a crucial piece of the annual FISMA evaluation. In addition to assessment and comments in key performance metric areas, OMB annual FISMA reporting guidance asks IGs to assess the quality of the agency POA&M process and C&A process, as well as the completeness of the agency system inventory. The Agency Head has the option to formally over-ride the IGs assessment of these metrics if he or she disagrees with their conclusions.

Agency CIOs manage the POA&M process for their agency. Program officials (e.g., system owners) must regularly (at least quarterly) update the CIO on their progress in implementing their own POA&Ms. This enables the CIO and IG to monitor agency-wide progress, identify problems, and provide accurate quarterly status updates to OMB.

[7] Memorandum from Clay Johnson to Heads of Agencies, May 19, 2006. "Where We'd Be Proud To Be on July 1, 2007."
[8] Id.

Table 2: Effectiveness of POA&M Process

OMB is responsible for tracking agency progress in resolving security deficiencies. Agency IGs were asked several questions to evaluate whether the agency maintains an effective plan of action and milestones process to remediate IT security weaknesses. To arrive at "Effective" as shown in this table, OMB considers a set of IG responses, including how weaknesses are incorporated in the POA&M, how they are prioritized, and how the status of weaknesses is tracked and reported.

Agency	Effective POA&M (Y/N)
Agency for International Development	Yes
Department of Agriculture	No
Department of Commerce	Yes
Department of Defense	No
Department of Education	Yes
Department of Energy	Yes
Environmental Protection Agency	Yes
General Services Administration	Yes
Department of Health and Human Services	Yes
Department of Homeland Security	No
Department of Housing and Urban Development	Yes
Department of the Interior	No
Department of Justice	Yes
Department of Labor	Yes
National Aeronautics and Space Administration	No
National Science Foundation	Yes
Nuclear Regulatory Commission	Yes
Office of Personnel Management	Yes
Small Business Administration	Yes
Smithsonian Institution	Yes
Social Security Administration	Yes
Department of State	Yes
Department of Transportation	Yes
Department of the Treasury	Yes
Department of Veterans Affairs	No
Total "Yes":	19
Total "No":	6

Table 3. Quality of Certification and Accreditation Processes
OMB is responsible for overseeing the effectiveness of agency security procedures. Agency IGs were asked to evaluate the quality of agency certification and accreditation processes. They were given response choices including: excellent, good, satisfactory, poor and failing.

Agency	Evaluation
Agency for International Development	Good
Department of Agriculture	Poor
Department of Commerce	Poor
Department of Defense	Poor
Department of Education	Satisfactory
Department of Energy	Poor
Environmental Protection Agency	Satisfactory
General Services Administration	Satisfactory
Department of Health and Human Services	Good
Department of Homeland Security	Satisfactory
Department of Housing and Urban Development	Satisfactory
Department of the Interior	Poor
Department of Justice	Good
Department of Labor	Good
National Aeronautics and Space Administration	Poor
National Science Foundation	Good
Nuclear Regulatory Commission	Failing
Office of Personnel Management	Excellent
Small Business Administration	Satisfactory
Smithsonian Institution	Satisfactory
Social Security Administration	Excellent
Department of State	Satisfactory
Department of Transportation	Good
Department of the Treasury	Poor
Department of Veterans Affairs	Poor
Total “Excellent”:	2
Total “Good”:	6
Total “Satisfactory”:	8
Total “Poor”:	8
Total “Failing”:	1

Table 4: System Inventory Completeness
OMB is responsible for ensuring agencies develop and maintain an inventory of major information systems. Agency IGs were asked to evaluate the extent to which an agency system inventory has been developed. They were given several response choices including: Approximately 0-50% complete, 51-70% complete, 71-80% complete, 81-95% complete, and 96-100% complete.

Agency	Evaluation
Agency for International Development	96-100%
Department of Agriculture	Unable to Determine
Department of Commerce	96-100%
Department of Defense	0-50%
Department of Education	96-100%
Department of Energy	81-95%
Environmental Protection Agency	96-100%
General Services Administration	96-100%
Department of Health and Human Services	96-100%
Department of Homeland Security	96-100%
Department of Housing and Urban Development	96-100%
Department of the Interior	96-100%
Department of Justice	96-100%
Department of Labor	96-100%
National Aeronautics and Space Administration	96-100%
National Science Foundation	96-100%
Nuclear Regulatory Commission	51-70%
Office of Personnel Management	96-100%
Small Business Administration	96-100%
Smithsonian Institution	96-100%
Social Security Administration	96-100%
Department of State	0-50%
Department of Transportation	96-100%
Department of the Treasury	51-70%
Department of Veterans Affairs	96-100%
Total “Approximately 96-100% complete”:	19
Total “Approximately 81-95% complete”:	1
Total “Approximately 71-80% complete”:	0
Total “Approximately 51-70% complete”:	2
Total "Approximately 0-50% complete":	2
Total “Unable to Determine”:	1

V. OMB Assessment of Agency Incident Handling Programs

A. Incident Reporting

FISMA requires each agency to document and implement procedures for detecting, reporting and responding to security incidents. Agencies must also notify and consult with US-CERT. The Act also requires OMB oversight of the US-CERT and NIST to issue incident detection and handling guidelines.[9]

By including these requirements, FISMA recognizes that the Federal government must protect its systems from external threats. While strong security controls can help reduce the number of successful attacks, experience shows that some attacks cannot be prevented. Consequently, an effective incident response capability is critical to the government-wide security program as well as individual agency programs.

In May 2005, DHS completed a Concept of Operations for Federal Cyber Security Incident Handling. This document was produced under the auspices of the Cyber Incident Response Policy Coordination Committee, co-chaired by OMB and the Homeland Security Council. Agencies' incident handling programs must follow the concept of operations when analyzing and reporting incident data.

The following information is excerpted from the US-CERT annual report for fiscal year 2006:

> During fiscal year 2006, federal agencies reported a record number of incidents to US-CERT. The trend shows a relatively stable reporting pattern for the first half of fiscal year 2006 with a noticeable increase in incidents reported in the second half, especially in the last two months of the fiscal year. A number of factors can be cited that resulted in changes in reporting patterns, including increased intrusion activity, and an Executive Order requiring the reporting of PII incidents to US-CERT.
>
> The largest risk for fiscal year 2006, seen across several incident categories, was the disclosure of PII. US-CERT saw a dramatic rise in fiscal year 2006 in incidents where either physical loss/theft or system compromise resulted in the loss of PII.

[9] In January 2004, NIST published SP 800-61 "Computer Security Incident Handling Guide." Per longstanding OMB policy, agencies are required to follow this and all other FISMA related NIST security guidance. This document discusses the establishment and maintenance of an effective incident response program. The guidelines include recommendations for handling certain types of incidents, such as distributed denial of service attacks and malicious code infections. In addition, the guidelines include a set of sample incident scenarios that can be used to perform incident response team exercises. The guidelines are technology neutral and can be followed regardless of hardware platform, operating system, protocol, or application.

US-CERT received daily reports of lost laptops, mobile devices, etc., throughout Q3 and Q4. US-CERT provided reports of all PII incidents to the Executive Office of the President within one hour in compliance with OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating Costs for Security in Agency Information Technology Investments." The rise in PII incidents included the increase in phishing scams, intended to steal PII data, such as fraudulent Katrina websites that targeted users and organizations alike.

In fiscal year 2006, 5146 incidents were reported to the DHS incident response center for six categories of incidents, a substantial increase in the number of incidents reported the prior year.

Table 5: Incident Reporting to US-CERT		
	FY 2005	**FY 2006**
Unauthorized Access	304	706
Denial of Service	31	37
Malicious Code	1,806	1,465
Improper Usage	370	638
Scans/Probes/Attempted Access	976	1,388
Investigation	82	912
Total Incidents Reported	3,569	5,146

- Unauthorized access. During fiscal year 2006, incidents involving unauthorized access were responsible for almost 14 percent of total incidents reported. The total number of incidents involving unauthorized access has more than doubled since fiscal year 2005. A further breakdown of this category shows that 50 percent of these incidents involved equipment loss or theft. Privileged or root system access accounted for 25 percent of unauthorized access incidents, which was more than double that of non-privileged access. An increased awareness of concerted intrusion efforts by hackers has led federal agencies to intensify their efforts to identify and report these incidents to US-CERT.

- Denial of service. During fiscal year 2006, denial of service incidents have increased by 20 percent. The total number of incidents still made up less than 1 percent of all incidents reported, which is consistent with the previous year's reporting.

- Malicious code. Incidents involving malicious code declined in fiscal year 2006 from the number reported in fiscal year 2005, the only category showing

a decrease. The decline came in both total numbers of incidents, and as a percentage of total incidents in all categories. The reason for this is probably two-fold—no major virus outbreaks of note in fiscal year 2006, and improvements in patching systems in a timely manner prevent vulnerabilities from being exploited.

- Improper Usage. During fiscal year 2006, incidents involving improper usage increased at a steady pace, with each quarter reporting more incidents than the previous quarter. Since there is no uniform acceptable use policy across the federal government, what constitutes a policy violation at one agency may not necessarily be a violation at another agency.

- Scans/probes/attempted access. During fiscal year 2006, the total number of scans, probes and attempted access incidents increased by 42 percent over the previous year; however, as a percentage of total incidents, it was practically unchanged. Quarter by quarter analysis shows a steady increase in reporting as the fiscal year progressed. The total number of incidents in Q4 was three times higher than in Q1.

- Investigation. These incidents are deemed by the reporting entity as unconfirmed and warranting further review as they are potentially malicious or anomalous. This category of incidents showed the largest increase of any category during fiscal year 2006. The total number of incidents filed increased by a staggering 11 fold, and comprised almost 18 percent of all incidents. The reason for this massive increase is intensive analysis of suspicious traffic picked up by the Einstein program sensors.[10] This has enabled US-CERT to identify potential malicious activity and to notify federal agencies of system compromise.

In order for DHS to successfully perform its duties, it must have an accurate depiction of incidents across all agency bureaus and operating divisions. Additionally, incident reports can provide CIOs and other senior managers with valuable input for risk assessments, help prioritize security improvements, and illustrate risk and related trends.

OMB will continue to work with agencies and DHS to ensure appropriate processes and procedures are in place to fully report on security incidents.

[10] The Einstein program provides a mechanism for the collection of summary network traffic information at agency gateways and provides a high level view across the federal government network infrastructure.

B. Incident Detection

Agencies must be able to quickly detect and respond to incidents. During the next year, OMB will work with federal agencies to increase the exchange of packet level (full content) information regarding incidents which have penetrated an agency's perimeter. Sharing this data will enable more effective analysis of attacks targeting multiple Federal agencies, and may enable more timely responses to new threats. The sharing of intrusion data will also improve the knowledge base of analysts in Federal agencies.

C. Incident Prevention

The threat to US Government systems is shifting from opportunistic hacking to targeted, dynamically adapting attacks. To counter this threat, agencies need to make the best use of existing IT security policies and practices. In addition, a long term architectural roadmap is necessary to provide a consistent strategy for mitigating malicious cyber activity.

NIST has produced comprehensive security guidance for agencies through the SP-800 series of publications. SP800-53 in particular includes very specific instruction around necessary security controls. Agencies should apply the NIST guidance using a baseline architectural roadmap that addresses not only the selection of security controls but the deployment and integration of those controls as part of a comprehensive framework of management, operational, and technical controls.

VI. Plan of Action to Improve Performance

A. President's Management Agenda Scorecard

While IT security clearly has a technical component, it is at its core an essential management function. OMB has increased executive level accountability for security and privacy by including these elements in the President's Management Agenda (PMA) scorecard.

The PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government). The goals of the E-Government initiative are to ensure the Federal government's annual investment in IT significantly improves the government's ability to serve citizens and to ensure systems are secure, delivered on time and on budget.

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of

performance in all the criteria), or red (agencies have any one of a number of serious flaws).

IT security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard, regardless of their performance against other E-Government criteria. Similarly, agencies must successfully meet information privacy components to maintain a green rating. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html.

To "get to green" under the E-Government Scorecard, agencies must meet the following three security criteria:

- IG or Agency Head verifies the effectiveness of the Department-wide IT security remediation process;
- IG or Agency Head rates the agency certification and accreditation process as "Satisfactory" or better; and
- The agency has 90 percent of all IT systems properly secured (certified and accredited).

In order to "maintain green," by July 1, 2007, agencies must meet the following security and privacy criteria:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations;
- Has demonstrated for 90 percent of applicable systems a PIA has been conducted and is publicly posted; and
- Has demonstrated for 90 percent of systems with PII contained in a system of records covered by the Privacy Act to have developed, published, and maintained a current SORN.

OMB will continue to use the E-Government scorecard to motivate agency managers and highlight areas for improvement.

B. Review of Agency Business Cases

OMB has integrated IT security and privacy into the capital planning and investment control process to promote greater attention to security and privacy as fundamental management priorities. To guide agency resource decisions and assist OMB oversight, OMB Circular A-11, "Preparation, Submission and Execution of the Budget," requires agencies to:

- Report security costs for all IT investments;
- Document adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case justification for major IT investments. In their justification, agencies must answer a series of security and privacy questions and describe how the investment meets the requirements of the FISMA, E-Government Act, Privacy Act, OMB policy, and NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

C. Information System Security Line of Business

The Information Systems Security Line of Business (ISS LOB) is an interagency effort to identify ways to make consistent and strengthen the ability of all agencies to identify and defend against threats, correct vulnerabilities, and manage risks. DHS serves as the managing agency for this line of business, which is part of the President's E-Government Initiatives.

The ISS LOB selected three agencies as shared service centers for security awareness training, DOD, the Office of Personnel Management, and DOS – in coordination with the United States Agency for International Development. Additionally, two agencies were selected as shared service centers for FISMA reporting, the Department of Justice and the Environmental Protection Agency. These agencies were selected through a competitive and analytically-derived process based on their qualifications and ability to provide information security products and services on a government-wide basis. Each shared service center has a business process in place to support cross-agency servicing, and agencies will now select their center and provide the ISS LOB with their plans to migrate to them. Shared service centers for security awareness training and FISMA reporting will begin operation in April 2007.

Shared service centers will eliminate the need for each agency to develop security awareness training or obtain an automated tool for managing their FISMA reporting on their own. This will maximize resources and result in standardized information security programs and better-trained workforces, cognizant of their information security responsibilities. It will also allow agencies to dedicate their limited resources to critical, mission-specific security issues. By providing shared solutions for common information security areas, the ISS LOB will allow all federal departments and agencies to benefit from improved levels of cyber security, reduced costs, elimination of duplicative efforts, and improved quality of service and expertise through specialization and consolidation.

VII. Agency Privacy Management

In 2006 several agencies experienced high profile data security breaches involving PII. Most notable of these is Veterans Affairs, but significant problems also exist at Commerce/Census Bureau, HUD, and others. DHS reports 15 agencies have reported to them 338 separate security incidents involving PII in this fiscal year. Virtually all of these incidents resulted from "internal" problems within agencies and not external attacks on agency systems.

To help address the above issues, in May the President signed Executive Order 13402, "Strengthening Federal Efforts to Protect Against Identity Theft," creating the Federal Identity Theft Task Force. Several of the Task Force's interim recommendations address the need to improve data security in the government, improve the agencies' ability to respond to data breaches, and reduce the risk to personal information.

Additionally, the General Service's Administration's SmartBUY program recently joined in partnership with the Department of Defense Enterprise Software Initiative to provide Government-wide contractual vehicles for Data at Rest (DAR) encryption commercial solutions to protect sensitive data. This partnership will establish agreements with several vendors to provide cost-effective tools for agencies to protect their information in support of OMB memorandum M-06-16, "Protection of Sensitive Agency Information."

OMB takes seriously its responsibility associated with upholding the legally embedded tenets of personal privacy and oversees these tenets through agency oversight, gathering of government-wide privacy and security program review, and agency-specific regulatory review. Through the Identity Theft Task Force, OMB is charged with developing government-wide policy to address breaches of personal information and breach notification. OMB endeavors to steward a common, risk-based approach to breaches to include notification and remediation, as well as privacy training and awareness for all federal employees.

In the context of the Identity Theft Task Force, OMB has issued four security and privacy policy and advisory memoranda. These memoranda reemphasize agency responsibilities under law and

policy regarding protection and safeguard of sensitive PII, including information accessed through removable media, and incident reporting.[11]

[11] To learn more about these policies, see: OMB Memorandum 06-15, "Safeguarding Personally Identifiable Information," OMB Memorandum 06-16, "Protection of Sensitive Agency Information," OMB Memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," and OMB Memorandum 06-20, "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," respectively.

VIII. Conclusion

Over the past year, agencies continued to make progress in closing the Federal government's IT security performance gaps in some areas. Analysis of baseline performance measures indicated security compliance improvements including a 10 percent increase in security awareness training for agency employees and contractors and a three percent increase in training for employees with significant information security responsibilities.

Table 6: Security Policy Compliance Improvements			
	FY 2005	**FY 2006**	**Increase**
Number of Reported Systems	10,239	10,600	3%
Number of Systems Certified and Accredited	8735	9313	6.6%
Number of Systems with Tested Contingency Plans	6233	8144	30%
Number of Systems with Tested Controls	7422	9312	25%

However, progress degraded slightly in other areas, with the downward trend primarily attributable to a few agencies rather than being a Government-wide pattern. Through existing processes, OMB will continue to work with agencies to focus management attention on:

- Accurate and up-to-date system inventories, security configurations, contingency plans, and contractor oversight;
- Agency certification and accreditation and POA&M processes;
- Agency determination and assignment of risk impact levels;
- General and job-specific privacy training for Federal employees and contractors;
- Oversight coordination between agencies and IGs; and
- PIA and SORN maintenance for 90 percent of applicable systems.

The Administration intends to focus on the implementation of the ISS LOB to increase security effectiveness and reduce costs across government. The establishment of shared service centers for security training and FISMA reporting is the first step towards ensuring greater use of standardized products and services.

OMB will continue to work with agencies, IGs, CIOs, GAO, and the Congress to strengthen the Federal government's IT security and privacy programs.

A copy of this report is available at www.whitehouse.gov/omb.

IX. Additional Information

Appendix A: Individual Agency Summaries
Appendix B: Reporting by Small and Independent Agencies
Appendix C: Federal Government IT Security Program

Appendix A: Individual Agency Summaries

In fiscal year 2006, agencies submitted FISMA reports, a corresponding evaluation by the agency IG or a designated independent assessor. This appendix includes a government-wide summary of agency CIO and IG reports, as well as detailed individual agency performance summaries.

Information is provided, at the agency specific level, on performance measures collected in the following categories:

- System Inventory Development and Verification.
- Certification and Accreditation;
- Testing of System Security Controls and Contingency Plans;
- Incident Reporting;
- Security Awareness, Training and Education;
- Configuration Management Policies;
- Agency Plan of Action and Milestones Process;
- Quality of the Certification and Accreditation Process;
- Documented Procedures for Using Emerging Technologies;
- Senior Agency Official for Privacy Responsibilities;
- Privacy Procedures and Practices;
- Privacy Impact Assessments and System of Records Notices; and
- Privacy Internal Oversight.

FY 2006 Government-wide Summary -- CIO Reports

Total Number of systems	**10,595**	
Agency systems	9,388	
High	1,367	
Moderate	3,174	
Low	4,516	
Not categorized	331	
Contractor systems	1,207	
High	236	
Moderate	397	
Low	205	
Not categorized	369	
Certified and Accredited Systems - Total	9,313	**88%**
High	1,433	89%
Moderate	3,186	89%
Low	4,050	86%
Not categorized	644	92%
Tested Security Controls - Total	9,312	**88%**
High	1,401	87%
Moderate	3,136	88%
Low	4,121	87%
Not categorized	654	93%
Tested Contingency Plans - Total	8,144	**77%**
High	1,026	64%
Moderate	2,837	79%
Low	3,792	80%
Not categorized	489	70%
Total # of Systems not Categorized	700	7%
Incidents Reported Internally	6,163,592	
Incidents Reported to USCERT	6,114,037	
Incidents Reported to Law Enforcement	899	
Total Number of Employees	3,847,006	
Employees that received IT security awareness training	3,491,290	91%
Total Number of Employees with significant IT security responsibilities	105,805	
Employees with significant responsibilities that received training	91,387	86%
Total Costs for providing IT security training	$74,132,579	

The agency explains policies regarding peer-to-peer file sharing in training	Yes	25 agencies
	No	0 agencies
There is an agency-wide security configuration policy	Yes	24 agencies
	No	1 agencies
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	21 agencies
	No	4 agencies

-This page left blank intentionally-

FY 2006 Government-wide Summary -- IG Reports

Quality of agency C&A process	Excellent	2 agencies
	Good	6 agencies
	Satisfactory	8 agencies
	Poor	8 agencies
	Failing	1 agencies
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance		
1 IG - unaudited (USDA)	Rarely (0-50% of the time)	3 agencies
	Sometimes (51-70% of the time)	3 agencies
	Frequently (71-80% of the time)	2 agencies
	Mostly (81-95% of the time)	1 agencies
	Almost Always (96-100% of the time)	15 agencies
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)		
1 IG - unaudited (USDA)	Approximately 0-50% complete	2 agencies
	Approximately 51-70% complete	2 agencies
	Approximately 71-80% complete	0 agencies
	Approximately 81-95% complete	2 agencies
	Approximately 96-100% complete	18 agencies
The OIG generally agrees with the CIO on the number of agency owned systems	Yes	22 agencies
	No	3 agencies
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes	22 agencies
	No	3 agencies
The agency inventory is maintained and updated at least annually	Yes	22 agencies
	No	3 agencies
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency		
1 IG - unaudited (USDA)	Rarely (0-50% of the time)	1 agencies
	Sometimes (51-70% of the time)	2 agencies
	Frequently (71-80% of the time)	4 agencies
	Mostly (81-95% of the time)	7 agencies
	Almost Always (96-100% of the time)	10 agencies
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time)	2 agencies
1 IG - unaudited (USDA)	Sometimes (51-70% of the time)	2 agencies
	Frequently (71-80% of the time)	1 agencies
	Mostly (81-95% of the time)	5 agencies
	Almost Always (96-100% of the time)	14 agencies

FY 2006 Government-wide Summary -- IG Reports (continued)

Effective POA&M process?	Yes	19 agencies
Note: To arrive at "Effective" as reflected in this Appendix, OMB considers a set of IG responses, including how weaknesses are incorporated in the POA&M, how they are prioritized, and how the status of weaknesses is tracked and reported.	No	6 agencies
The agency has completed system e-authentication risk assessments	Yes	18 agencies
	No	7 agencies
There is an agency wide security configuration policy	Yes	22 agencies
	No	3 agencies
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes	21 agencies
1 IG - Unaudited (DoD)	No	3 agencies
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes	22 agencies
1 IG - Unaudited (DoD)	No	2 agencies
The agency follows defined procedures for reporting to the USCERT	Yes	23 agencies
1 IG - Unaudited (DoD)	No	1 agencies

The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Rarely (0-50% of employees)	1 agencies
	Sometimes (51-70% of employees)	1 agencies
	Frequently (71-80% of employees)	4 agencies
	Mostly (81-95% of employees)	8 agencies
	Almost Always (96-100% of employees)	11 agencies

The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes	25 agencies
	No	0 agencies

FY 2006 Government-wide Summary -- Privacy Reports

Systems that contain Federally-owned information in identifiable form	**2,870**			
Agency	2,524			
Contractor	346			
Systems requiring a Privacy Impact Assessment	**1,321**			
Agency	1,213			
Contractor	108			
Systems that have complete and current Privacy Impact Assessment	**1,113**			84%
Agency	1,018			
Contractor	95			
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**1,874**			
Agency	1,665			
Contractor	209			
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**1,555**			83%
Agency	1,363			
Contractor	192			
The privacy official participates in all agency information privacy compliance activities.		Yes	25 agencies	
		No	0 agencies	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.		Yes	24 agencies	
		No	1 agencies	
The privacy official participates in assessing the impact of technology on the privacy of personal information.		Yes	25 agencies	
		No	0 agencies	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?		Yes	23 agencies	
		No	2 agencies	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.		Yes	21 agencies	
		No	4 agencies	

FY 2006 Government-wide Summary -- Privacy Reports (continued)

The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	22 agencies
	No	3 agencies
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	22 agencies
	No	3 agencies
Public-facing agency web sites have machine-readable privacy policies.	Yes	23 agencies
	No	2 agencies
Agency uses persistent tracking technology on any web site.	Yes	8 agencies
	No	17 agencies
Agency annually reviews the use of persistent tracking.	Yes	17 agencies
	No	8 agencies
Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes	23 agencies
	No	2 agencies
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes	22 agencies
	No	3 agencies
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices.	Yes	14 agencies
	No	11 agencies
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:		
Compilation of agency's privacy and data protection policies and procedures	Yes	22 agencies
	No	3 agencies
Summary of the agency's use of information in identifiable form	Yes	21 agencies
	No	4 agencies
Verification of intent to comply with agency policies and procedures	Yes	22 agencies
	No	3 agencies
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes	9 agencies
	No	16 agencies

US Agency for International Development -- CIO Report

Total Number of Systems	**11**	
Agency Systems	**8**	
High	0	
Moderate	5	
Low	3	
Not categorized	0	
Contractor Systems	**3**	
High	0	
Moderate	3	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	11	100%
High	0	0%
Moderate	8	100%
Low	3	100%
Not categorized	0	0%
Tested Security Controls - Total	11	100%
High	0	0%
Moderate	8	100%
Low	3	100%
Not categorized	0	0%
Tested Contingency Plans - Total	11	100%
High	0	0%
Moderate	8	100%
Low	3	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	75	
Incidents Reported to USCERT	75	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	8,417	
Employees that received IT security awareness training	8,417	100%
Total Number of Employees w/significant IT security responsibilities	194	
Employees with significant responsibilities that received training	182	94%
Total Costs for providing IT security training	$30,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

US Agency for International Development -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

US Agency for International Development -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**2**	
Agency	2	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**2**	
Agency	2	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**2**	100%
Agency	2	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**0**	
Agency	0	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**0**	0%
Agency	0	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

US Agency for International Development -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of Agriculture -- CIO Report

Total Number of Systems	**258**	
Agency Systems	**253**	
High	40	
Moderate	146	
Low	58	
Not categorized	9	
Contractor Systems	**5**	
High	1	
Moderate	4	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	242	94%
High	40	98%
Moderate	146	97%
Low	56	97%
Not categorized	0	0%
Tested Security Controls - Total	241	93%
High	41	100%
Moderate	144	96%
Low	56	97%
Not categorized	0	0%
Tested Contingency Plans - Total	237	92%
High	40	98%
Moderate	141	94%
Low	56	97%
Not categorized	0	0%
Total # of Systems not Categorized	9	
Incidents Reported Internally	126	
Incidents Reported to USCERT	101	
Incidents Reported to Law Enforcement	2	
Total Number of Employees	111,476	
Employees that received IT security awareness training	110,019	99%
Total Number of Employees w/significant IT security responsibilities	1,526	
Employees with significant responsibilities that received training	1,526	100%
Total Costs for providing IT security training	$435,542	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Agriculture -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Unable to answer
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Unable to answer
The OIG generally agrees with the CIO on the number of agency owned systems	No
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Unable to answer
OIG Findings are incorporated into the POA&M process	Unable to answer
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	No
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Agriculture -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**135**	
Agency	134	
Contractor	1	
Systems requiring a Privacy Impact Assessment	**88**	
Agency	87	
Contractor	1	
Systems that have complete and current Privacy Impact Assessment	**112**	127%
Agency	111	* see footnote next pg
Contractor	1	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**91**	
Agency	90	
Contractor	1	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**83**	91%
Agency	83	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	No	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Department of Agriculture -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

* Some agencies interpret the question regarding total number of systems requiring a PIA as two discrete steps: 1) initial analysis of information maintained in all systems; and, when necessary 2) completion of a full PIA when required under the E-Government Act. Agencies who interpret the question in this manner may have percentages of greater than 100%.

Department of Commerce -- CIO Report

Total Number of Systems	**318**	
Agency Systems	**306**	
High	24	
Moderate	193	
Low	76	
Not categorized	13	
Contractor Systems	**12**	
High	3	
Moderate	9	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	294	92%
High	24	89%
Moderate	184	91%
Low	73	96%
Not categorized	13	100%
Tested Security Controls - Total	266	84%
High	15	56%
Moderate	172	85%
Low	67	88%
Not categorized	12	92%
Tested Contingency Plans - Total	252	79%
High	24	89%
Moderate	172	85%
Low	50	66%
Not categorized	6	46%
Total # of Systems not Categorized	13	
Incidents Reported Internally	590	
Incidents Reported to USCERT	290	
Incidents Reported to Law Enforcement	252	
Total Number of Employees	45,033	
Employees that received IT security awareness training	44,049	98%
Total Number of Employees w/significant IT security responsibilities	1,362	
Employees with significant responsibilities that received training	930	68%
Total Costs for providing IT security training	$1,110,500	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Commerce -- IG Report

Quality of agency C&A process (includes USPTO)	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Commerce -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**37**	
Agency	37	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**34**	
Agency	34	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**34**	100%
Agency	34	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**37**	
Agency	37	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**37**	100%
Agency	37	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Commerce -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of Defense -- CIO Report

Total Number of Systems	**4139**	
Agency Systems	**4079**	
High	329	
Moderate	907	
Low	2780	
Not categorized	63	
Contractor Systems	**60**	
High	1	
Moderate	15	
Low	44	
Not categorized	0	
Certified and Accredited Systems - Total	3360	81%
High	270	82%
Moderate	759	82%
Low	2286	81%
Not categorized	45	71%
Tested Security Controls - Total	3617	87%
High	297	90%
Moderate	804	87%
Low	2476	88%
Not categorized	40	63%
Tested Contingency Plans - Total	3458	84%
High	281	85%
Moderate	753	82%
Low	2411	85%
Not categorized	13	21%
Total # of Systems not Categorized	63	
Incidents Reported Internally	21772	
Incidents Reported to USCERT	21772	
Incidents Reported to Law Enforcement	53	
Total Number of Employees	2,338,146	
Employees that received IT security awareness training	2,068,594	88%
Total Number of Employees w/significant IT security responsibilities	70,767	
Employees with significant responsibilities that received training	60,955	86%
Total Costs for providing IT security training	$38,084,955	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Defense -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 0-50% complete
The OIG generally agrees with the CIO on the number of agency owned systems	No
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	No
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Rarely (0-50% of the time)
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Unaudited
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Unaudited
The agency follows defined procedures for reporting to the USCERT	Unaudited
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Sometimes (51-70% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Defense -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**458**	
Agency	450	
Contractor	8	
Systems requiring a Privacy Impact Assessment	**195**	
Agency	194	
Contractor	1	
Systems that have complete and current Privacy Impact Assessment	**73**	37%
Agency	72	
Contractor	1	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**333**	
Agency	330	
Contractor	3	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**97**	29%
Agency	97	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Defense -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of Education -- CIO Report

Total Number of Systems	**146**	
Agency Systems	**92**	
High	4	
Moderate	36	
Low	52	
Not categorized	0	
Contractor Systems	**54**	
High	2	
Moderate	25	
Low	27	
Not categorized	0	
Certified and Accredited Systems - Total	128	88%
High	6	100%
Moderate	55	90%
Low	67	85%
Not categorized	0	0%
Tested Security Controls - Total	134	92%
High	6	100%
Moderate	60	98%
Low	68	86%
Not categorized	0	0%
Tested Contingency Plans - Total	44	30%
High	6	100%
Moderate	38	62%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	421	
Incidents Reported to USCERT	54	
Incidents Reported to Law Enforcement	54	
Total Number of Employees	10,405	
Employees that received IT security awareness training	10,342	99%
Total Number of Employees w/significant IT security responsibilities	1,046	
Employees with significant responsibilities that received training	965	92%
Total Costs for providing IT security training	$411,178	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of Education -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Education -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**83**	
Agency	42	
Contractor	41	
Systems requiring a Privacy Impact Assessment	**16**	
Agency	3	
Contractor	13	
Systems that have complete and current Privacy Impact Assessment	**15**	94%
Agency	3	
Contractor	12	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**83**	
Agency	42	
Contractor	41	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**83**	100%
Agency	42	
Contractor	41	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	No	

Department of Education -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	No
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of Energy -- CIO Report

Total Number of Systems	**817**	
Agency Systems	**187**	
High	32	
Moderate	87	
Low	44	
Not categorized	24	
Contractor Systems	**630**	
High	123	
Moderate	93	
Low	58	
Not categorized	356	
Certified and Accredited Systems - Total	815	100%
High	155	100%
Moderate	180	100%
Low	100	98%
Not categorized	380	100%
Tested Security Controls - Total	722	88%
High	85	55%
Moderate	172	96%
Low	86	84%
Not categorized	379	100%
Tested Contingency Plans - Total	698	85%
High	124	80%
Moderate	163	91%
Low	87	85%
Not categorized	324	85%
Total # of Systems not Categorized	380	
Incidents Reported Internally	115	
Incidents Reported to USCERT	115	
Incidents Reported to Law Enforcement	115	
Total Number of Employees	140,513	
Employees that received IT security awareness training	136,111	97%
Total Number of Employees w/significant IT security responsibilities	3,685	
Employees with significant responsibilities that received training	3,223	87%
Total Costs for providing IT security training	$10,552,764	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of Energy -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 81-95% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	No
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Energy -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**187**	
Agency	72	
Contractor	115	
Systems requiring a Privacy Impact Assessment	**23**	
Agency	17	
Contractor	6	
Systems that have complete and current Privacy Impact Assessment	**22**	96%
Agency	18	
Contractor	4	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**66**	
Agency	45	
Contractor	21	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**66**	100%
Agency	45	
Contractor	21	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	No	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Department of Energy -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Environmental Protection Agency -- CIO Report

Total Number of Systems	**173**	
Agency Systems	**159**	
High	4	
Moderate	111	
Low	44	
Not categorized	0	
Contractor Systems	**14**	
High	0	
Moderate	8	
Low	6	
Not categorized	0	
Certified and Accredited Systems - Total	173	100%
High	4	100%
Moderate	119	100%
Low	50	100%
Not categorized	0	0%
Tested Security Controls - Total	173	100%
High	4	100%
Moderate	119	100%
Low	50	100%
Not categorized	0	0%
Tested Contingency Plans - Total	173	100%
High	4	100%
Moderate	119	100%
Low	50	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	494	
Incidents Reported to USCERT	360	
Incidents Reported to Law Enforcement	8	
Total Number of Employees	20,618	
Employees that received IT security awareness training	20,618	100%
Total Number of Employees w/significant IT security responsibilities	568	
Employees with significant responsibilities that received training	522	92%
Total Costs for providing IT security training	$614,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Environmental Protection Agency -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Environmental Protection Agency -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**29**	
Agency	1	
Contractor	28	
Systems requiring a Privacy Impact Assessment	**6**	
Agency	0	
Contractor	6	
Systems that have complete and current Privacy Impact Assessment	**3**	50%
Agency	0	
Contractor	3	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**43**	
Agency	0	
Contractor	43	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**43**	100%
Agency	0	
Contractor	43	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	No	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	No	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	No	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Environmental Protection Agency -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	No
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	No
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

General Services Administration -- CIO Report

Total Number of Systems	**79**	
Agency Systems	**44**	
High	0	
Moderate	35	
Low	9	
Not categorized	0	
Contractor Systems	**35**	
High	0	
Moderate	23	
Low	12	
Not categorized	0	
Certified and Accredited Systems - Total	79	100%
High	0	0%
Moderate	58	100%
Low	21	100%
Not categorized	0	0%
Tested Security Controls - Total	79	100%
High	0	0%
Moderate	58	100%
Low	21	100%
Not categorized	0	0%
Tested Contingency Plans - Total	79	100%
High	0	0%
Moderate	58	100%
Low	21	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	21	
Incidents Reported to USCERT	21	
Incidents Reported to Law Enforcement	4	
Total Number of Employees	15,111	
Employees that received IT security awareness training	15,111	100%
Total Number of Employees w/significant IT security responsibilities	975	
Employees with significant responsibilities that received training	972	100%
Total Costs for providing IT security training	$150,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

General Services Administration -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

General Services Administration -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**39**	
Agency	28	
Contractor	11	
Systems requiring a Privacy Impact Assessment	**15**	
Agency	5	
Contractor	10	
Systems that have complete and current Privacy Impact Assessment	**15**	100%
Agency	5	
Contractor	10	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**39**	
Agency	28	
Contractor	11	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**36**	92%
Agency	26	
Contractor	10	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	No	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

General Services Administration -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of Health and Human Services -- CIO Report

Total Number of Systems	**158**	
Agency Systems	**141**	
High	44	
Moderate	83	
Low	14	
Not categorized	0	
Contractor Systems	**17**	
High	6	
Moderate	4	
Low	7	
Not categorized	0	
Certified and Accredited Systems - Total	158	100%
High	50	100%
Moderate	87	100%
Low	21	100%
Not categorized	0	0%
Tested Security Controls - Total	158	100%
High	50	100%
Moderate	87	100%
Low	21	100%
Not categorized	0	0%
Tested Contingency Plans - Total	158	100%
High	50	100%
Moderate	87	100%
Low	21	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	72	
Incidents Reported to USCERT	51	
Incidents Reported to Law Enforcement	15	
Total Number of Employees	86,383	
Employees that received IT security awareness training	85,690	99%
Total Number of Employees w/significant IT security responsibilities	3,643	
Employees with significant responsibilities that received training	3,597	99%
Total Costs for providing IT security training	$2,423,731	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Health and Human Services -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Health and Human Services -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**83**	
Agency	75	
Contractor	8	
Systems requiring a Privacy Impact Assessment	**158**	
Agency	141	
Contractor	17	
Systems that have complete and current Privacy Impact Assessment	**158**	100%
Agency	141	
Contractor	17	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**65**	
Agency	59	
Contractor	6	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**69**	106%
Agency	64	
Contractor	5	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Health and Human Services -- Privacy (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of Homeland Security -- CIO Report

Total Number of Systems	**692**	
Agency Systems	**486**	
High	256	
Moderate	186	
Low	43	
Not categorized	1	
Contractor Systems	**206**	
High	77	
Moderate	98	
Low	30	
Not categorized	1	
Certified and Accredited Systems - Total	589	85%
High	296	89%
Moderate	239	84%
Low	54	74%
Not categorized	0	0%
Tested Security Controls - Total	613	89%
High	304	91%
Moderate	247	87%
Low	61	84%
Not categorized	1	50%
Tested Contingency Plans - Total	413	60%
High	154	46%
Moderate	208	73%
Low	51	70%
Not categorized	0	0%
Total # of Systems not Categorized	2	
Incidents Reported Internally	326	
Incidents Reported to USCERT	326	
Incidents Reported to Law Enforcement	26	
Total Number of Employees	207,776	
Employees that received IT security awareness training	155,212	75%
Total Number of Employees w/significant IT security responsibilities	1,277	
Employees with significant responsibilities that received training	1,283	100%
Total Costs for providing IT security training	$2,276,002	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Homeland Security -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Homeland Security -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**347**	
Agency	342	
Contractor	5	
Systems requiring a Privacy Impact Assessment	**143**	
Agency	142	
Contractor	1	
Systems that have complete and current Privacy Impact Assessment	**34**	24%
Agency	34	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**12**	
Agency	12	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**12**	100%
Agency	12	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	No	
Public-facing agency web sites have machine-readable privacy policies.	No	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Homeland Security -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of Housing and Urban Development -- CIO Report

Total Number of Systems	**106**	
Agency Systems	**92**	
High	31	
Moderate	41	
Low	20	
Not categorized	0	
Contractor Systems	**14**	
High	1	
Moderate	12	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	106	100%
High	32	100%
Moderate	53	100%
Low	21	100%
Not categorized	0	0%
Tested Security Controls - Total	106	100%
High	32	100%
Moderate	53	100%
Low	21	100%
Not categorized	0	0%
Tested Contingency Plans - Total	106	100%
High	32	100%
Moderate	53	100%
Low	21	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	7	
Incidents Reported to USCERT	7	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	8,518	
Employees that received IT security awareness training	8,236	97%
Total Number of Employees w/significant IT security responsibilities	504	
Employees with significant responsibilities that received training	487	97%
Total Costs for providing IT security training	$60,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Housing and Urban Development -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Housing and Urban Development -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**82**	
Agency	82	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**13**	
Agency	13	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**33**	254%
Agency	33	*see footnote next pg
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**37**	
Agency	37	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**37**	100%
Agency	37	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Department of Housing and Urban Development -- Privacy (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	No
Summary of the agency's use of information in identifiable form	No
Verification of intent to comply with agency policies and procedures	No
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

* Some agencies interpret the question regarding total number of systems requiring a PIA as two discrete steps: 1) initial analysis of information maintained in all systems; and, when necessary 2) completion of a full PIA when required under the E-Government Act. Agencies who interpret the question in this manner may have percentages of greater than 100%.

Department of the Interior -- CIO Report

Total Number of Systems	**175**	
Agency Systems	**164**	
High	6	
Moderate	128	
Low	30	
Not categorized	0	
Contractor Systems	**11**	
High	0	
Moderate	9	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	171	98%
High	6	100%
Moderate	134	98%
Low	31	97%
Not categorized	0	0%
Tested Security Controls - Total	167	95%
High	6	100%
Moderate	130	95%
Low	31	97%
Not categorized	0	0%
Tested Contingency Plans - Total	163	93%
High	6	100%
Moderate	126	92%
Low	31	97%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	147	
Incidents Reported to USCERT	99	
Incidents Reported to Law Enforcement	46	
Total Number of Employees	73,857	
Employees that received IT security awareness training	72,621	98%
Total Number of Employees w/significant IT security responsibilities	2,575	
Employees with significant responsibilities that received training	1,583	61%
Total Costs for providing IT security training	$998,272	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of the Interior -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Frequently (71-80% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of the Interior -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**76**	
Agency	69	
Contractor	7	
Systems requiring a Privacy Impact Assessment	**53**	
Agency	49	
Contractor	4	
Systems that have complete and current Privacy Impact Assessment	**53**	100%
Agency	49	
Contractor	4	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**51**	
Agency	46	
Contractor	5	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**50**	98%
Agency	45	
Contractor	5	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

Department of the Interior -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of Justice -- CIO Report

Total Number of Systems	**219**	
Agency Systems	**207**	
High	82	
Moderate	80	
Low	45	
Not categorized	0	
Contractor Systems	**12**	
High	3	
Moderate	7	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	219	100%
High	85	100%
Moderate	87	100%
Low	47	100%
Not categorized	0	0%
Tested Security Controls - Total	219	100%
High	85	100%
Moderate	87	100%
Low	47	100%
Not categorized	0	0%
Tested Contingency Plans - Total	219	100%
High	85	100%
Moderate	87	100%
Low	47	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	1719	
Incidents Reported to USCERT	1705	
Incidents Reported to Law Enforcement	98	
Total Number of Employees	123,104	
Employees that received IT security awareness training	117,688	96%
Total Number of Employees w/significant IT security responsibilities	5,334	
Employees with significant responsibilities that received training	3,916	73%
Total Costs for providing IT security training	$3,053,048	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Justice -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Justice -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**158**	
Agency	149	
Contractor	9	
Systems requiring a Privacy Impact Assessment	**52**	
Agency	47	
Contractor	5	
Systems that have complete and current Privacy Impact Assessment	**45**	87%
Agency	40	
Contractor	5	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**120**	
Agency	112	
Contractor	8	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**118**	98%
Agency	110	
Contractor	8	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Justice -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of Labor -- CIO Report

Total Number of Systems	**85**	
Agency Systems	**76**	
High	0	
Moderate	64	
Low	12	
Not categorized	0	
Contractor Systems	**9**	
High	0	
Moderate	7	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Tested Security Controls - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Tested Contingency Plans - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	54	
Incidents Reported to USCERT	22	
Incidents Reported to Law Enforcement	10	
Total Number of Employees	17,646	
Employees that received IT security awareness training	16,972	96%
Total Number of Employees w/significant IT security responsibilities	638	
Employees with significant responsibilities that received training	576	90%
Total Costs for providing IT security training	$149,038	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Labor -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Labor -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**185**	
Agency	169	
Contractor	16	
Systems requiring a Privacy Impact Assessment	**39**	
Agency	36	
Contractor	3	
Systems that have complete and current Privacy Impact Assessment	**39**	100%
Agency	36	
Contractor	3	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**154**	
Agency	142	
Contractor	12	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**149**	97%
Agency	137	
Contractor	12	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Labor -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

National Aeronautics and Space Administration -- CIO Report

Total Number of Systems	**974**	
Agency Systems	**939**	
High	68	
Moderate	258	
Low	613	
Not categorized	0	
Contractor Systems	**35**	
High	7	
Moderate	23	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	747	77%
High	24	32%
Moderate	183	65%
Low	540	87%
Not categorized	0	0%
Tested Security Controls - Total	837	86%
High	55	73%
Moderate	225	80%
Low	557	90%
Not categorized	0	0%
Tested Contingency Plans - Total	835	86%
High	58	77%
Moderate	221	79%
Low	556	90%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	106	
Incidents Reported to USCERT	99	
Incidents Reported to Law Enforcement	99	
Total Number of Employees	60,745	
Employees that received IT security awareness training	56,109	92%
Total Number of Employees w/significant IT security responsibilities	2,815	
Employees with significant responsibilities that received training	2,613	93%
Total Costs for providing IT security training	$1,200,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Aeronautics and Space Administration -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

National Aeronautics and Space Administration -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**56**	
Agency	11	
Contractor	45	
Systems requiring a Privacy Impact Assessment	**10**	
Agency	0	
Contractor	10	
Systems that have complete and current Privacy Impact Assessment	**10**	100%
Agency	0	
Contractor	10	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**25**	
Agency	7	
Contractor	18	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**23**	92%
Agency	7	
Contractor	16	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	No	
The agency has written processes or policies for all listed aspects of Privacy Impact Assessments.	No	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	No	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

National Aeronautics and Space Administration -- Privacy (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	No
Summary of the agency's use of information in identifiable form	No
Verification of intent to comply with agency policies and procedures	No
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

National Science Foundation -- CIO Report

Total Number of Systems	**19**	
Agency Systems	**16**	
High	4	
Moderate	8	
Low	4	
Not categorized	0	
Contractor Systems	**3**	
High	2	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Security Controls - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Contingency Plans - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	2	
Incidents Reported to USCERT	2	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	4,582	
Employees that received IT security awareness training	4,431	97%
Total Number of Employees w/significant IT security responsibilities	84	
Employees with significant responsibilities that received training	84	100%
Total Costs for providing IT security training	$77,500	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Science Foundation -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

National Science Foundation -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**2**	
Agency	2	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**2**	
Agency	2	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**2**	100%
Agency	2	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**2**	
Agency	2	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**2**	100%
Agency	2	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

National Science Foundation -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Nuclear Regulatory Commission -- CIO Report

Total Number of Systems	**43**	
Agency Systems	**31**	
High	3	
Moderate	8	
Low	0	
Not categorized	20	
Contractor Systems	**12**	
High	0	
Moderate	0	
Low	1	
Not categorized	11	
Certified and Accredited Systems - Total	5	12%
High	0	0%
Moderate	0	0%
Low	0	0%
Not categorized	5	16%
Tested Security Controls - Total	33	77%
High	3	100%
Moderate	8	100%
Low	1	100%
Not categorized	21	68%
Tested Contingency Plans - Total	4	9%
High	0	0%
Moderate	3	38%
Low	1	100%
Not categorized	0	0%
Total # of Systems not Categorized	31	
Incidents Reported Internally	47681	
Incidents Reported to USCERT	25	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	3,712	
Employees that received IT security awareness training	3,670	99%
Total Number of Employees w/significant IT security responsibilities	115	
Employees with significant responsibilities that received training	80	70%
Total Costs for providing IT security training	$315,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Nuclear Regulatory Commission -- IG Report

Quality of agency C&A process	Failing
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 51-70% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Nuclear Regulatory Commission -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**84**	
Agency	74	
Contractor	10	
Systems requiring a Privacy Impact Assessment	**29**	
Agency	22	
Contractor	7	
Systems that have complete and current Privacy Impact Assessment	**14**	48%
Agency	12	
Contractor	2	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**38**	
Agency	29	
Contractor	9	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**37**	97%
Agency	29	
Contractor	8	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Nuclear Regulatory Commission -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	No
Summary of the agency's use of information in identifiable form	No
Verification of intent to comply with agency policies and procedures	No
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Office of Personnel Management -- CIO Report

Total Number of Systems	**38**	
Agency Systems	**33**	
High	6	
Moderate	25	
Low	2	
Not categorized	0	
Contractor Systems	**5**	
High	1	
Moderate	3	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	38	100%
High	7	100%
Moderate	28	100%
Low	3	100%
Not categorized	0	0%
Tested Security Controls - Total	38	100%
High	7	100%
Moderate	28	100%
Low	3	100%
Not categorized	0	0%
Tested Contingency Plans - Total	38	100%
High	7	100%
Moderate	28	100%
Low	3	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	4	
Incidents Reported to USCERT	4	
Incidents Reported to Law Enforcement	1	
Total Number of Employees	5,165	
Employees that received IT security awareness training	5,165	100%
Total Number of Employees w/significant IT security responsibilities	83	
Employees with significant responsibilities that received training	82	99%
Total Costs for providing IT security training	$101,712	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Office of Personnel Management -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Office of Personnel Management -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**36**	
Agency	32	
Contractor	4	
Systems requiring a Privacy Impact Assessment	**28**	
Agency	26	
Contractor	2	
Systems that have complete and current Privacy Impact Assessment	**16**	57%
Agency	14	
Contractor	2	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**36**	
Agency	32	
Contractor	4	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**36**	100%
Agency	32	
Contractor	4	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	No	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	No	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Office of Personnel Management -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Small Business Administration -- CIO Report

Total Number of Systems	**19**	
Agency Systems	**13**	
High	2	
Moderate	11	
Low	0	
Not categorized	0	
Contractor Systems	**6**	
High	3	
Moderate	3	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	19	100%
High	5	100%
Moderate	14	100%
Low	0	0%
Not categorized	0	0%
Tested Security Controls - Total	19	100%
High	5	100%
Moderate	14	100%
Low	0	0%
Not categorized	0	0%
Tested Contingency Plans - Total	19	100%
High	5	100%
Moderate	14	100%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	6087955	
Incidents Reported to USCERT	6087955	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	6,522	
Employees that received IT security awareness training	4,851	74%
Total Number of Employees w/significant IT security responsibilities	283	
Employees with significant responsibilities that received training	237	84%
Total Costs for providing IT security training	$20,300	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Small Business Administration -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Small Business Administration -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**19**	
Agency	14	
Contractor	5	
Systems requiring a Privacy Impact Assessment	**19**	
Agency	14	
Contractor	5	
Systems that have complete and current Privacy Impact Assessment	**19**	100%
Agency	14	
Contractor	5	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**19**	
Agency	14	
Contractor	5	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**19**	100%
Agency	14	
Contractor	5	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	Yes	

Small Business Administration -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Smithsonian Institution -- CIO Report

Total Number of Systems	**18**	
Agency Systems	**17**	
High	0	
Moderate	6	
Low	11	
Not categorized	0	
Contractor Systems	**1**	
High	0	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	17	94%
High	0	0%
Moderate	6	86%
Low	11	100%
Not categorized	0	0%
Tested Security Controls - Total	18	100%
High	0	0%
Moderate	7	100%
Low	11	100%
Not categorized	0	0%
Tested Contingency Plans - Total	18	100%
High	0	0%
Moderate	7	100%
Low	11	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	3	
Incidents Reported to USCERT	3	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	7,500	
Employees that received IT security awareness training	7,089	95%
Total Number of Employees w/significant IT security responsibilities	144	
Employees with significant responsibilities that received training	23	16%
Total Costs for providing IT security training	$4,658	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Smithsonian Institution -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Frequently (71-80% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Smithsonian Institution -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**15**	
Agency	14	
Contractor	1	
Systems requiring a Privacy Impact Assessment	**12**	
Agency	11	
Contractor	1	
Systems that have complete and current Privacy Impact Assessment	**12**	100%
Agency	11	
Contractor	1	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**0**	
Agency	0	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**0**	0%
Agency	0	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	No	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Smithsonian Institution -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	No
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	No
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	No
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	No
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Social Security Administration -- CIO Report

Total Number of Systems	**20**	
Agency Systems	**20**	
High	0	
Moderate	8	
Low	12	
Not categorized	0	
Contractor Systems	**0**	
High	0	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Tested Security Controls - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Tested Contingency Plans - Total	20	100%
High	0	0%
Moderate	8	100%
Low	12	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	3	
Incidents Reported to USCERT	1	
Incidents Reported to Law Enforcement	3	
Total Number of Employees	65,236	
Employees that received IT security awareness training	65,236	100%
Total Number of Employees w/significant IT security responsibilities	442	
Employees with significant responsibilities that received training	409	93%
Total Costs for providing IT security training	$368,810	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Social Security Administration -- IG Report

Quality of agency C&A process	Excellent
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Social Security Administration -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**18**	
Agency	18	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**18**	
Agency	0	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**18**	100%
Agency	18	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**18**	
Agency	18	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**18**	100%
Agency	18	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Social Security Administration -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Department of State -- CIO Report

Total Number of Systems	**281**	
Agency Systems	**255**	
High	35	
Moderate	104	
Low	116	
Not categorized	0	
Contractor Systems	**26**	
High	0	
Moderate	24	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	256	91%
High	33	94%
Moderate	108	84%
Low	115	97%
Not categorized	0	0%
Tested Security Controls - Total	83	30%
High	12	34%
Moderate	38	30%
Low	33	28%
Not categorized	0	0%
Tested Contingency Plans - Total	162	58%
High	24	69%
Moderate	85	66%
Low	53	45%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	6	
Incidents Reported to USCERT	3	
Incidents Reported to Law Enforcement	5	
Total Number of Employees	52,913	
Employees that received IT security awareness training	52,913	100%
Total Number of Employees w/significant IT security responsibilities	2,132	
Employees with significant responsibilities that received training	1,618	76%
Total Costs for providing IT security training	$2,976,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of State -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 0-50% complete
The OIG generally agrees with the CIO on the number of agency owned systems	No
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	No
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Frequently (71-80% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of State -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**58**	
Agency	58	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**39**	
Agency	39	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**59**	151%
Agency	59	*See footnote next pg
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**59**	
Agency	59	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**59**	100%
Agency	59	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	No	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	No	

Department of State -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

* Some agencies interpret the question regarding total number of systems requiring a PIA as two discrete steps: 1) initial analysis of information maintained in all systems; and, when necessary 2) completion of a full PIA when required under the E-Government Act. Agencies who interpret the question in this manner may have percentages of greater than 100%.

Department of Transportation -- CIO Report

Total Number of Systems	**426**	
Agency Systems	**410**	
High	41	
Moderate	254	
Low	115	
Not categorized	0	
Contractor Systems	**16**	
High	0	
Moderate	13	
Low	3	
Not categorized	0	
Certified and Accredited Systems - Total	425	100%
High	41	100%
Moderate	266	100%
Low	118	100%
Not categorized	0	0%
Tested Security Controls - Total	417	98%
High	41	100%
Moderate	260	97%
Low	116	98%
Not categorized	0	0%
Tested Contingency Plans - Total	221	52%
High	18	44%
Moderate	147	55%
Low	56	47%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	1403	
Incidents Reported to USCERT	667	
Incidents Reported to Law Enforcement	6	
Total Number of Employees	73,561	
Employees that received IT security awareness training	66,706	91%
Total Number of Employees w/significant IT security responsibilities	1,276	
Employees with significant responsibilities that received training	1,232	97%
Total Costs for providing IT security training	$1,577,443	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Transportation -- IG Report

Quality of agency C&A process	Good
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Transportation -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**103**	
Agency	83	
Contractor	20	
Systems requiring a Privacy Impact Assessment	**42**	
Agency	35	
Contractor	7	
Systems that have complete and current Privacy Impact Assessment	**35**	83%
Agency	28	
Contractor	7	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**75**	
Agency	62	
Contractor	13	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**69**	92%
Agency	57	
Contractor	12	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Transportation -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of the Treasury -- CIO Report

Total Number of Systems	**786**	
Agency Systems	**770**	
High	47	
Moderate	328	
Low	194	
Not categorized	201	
Contractor Systems	**16**	
High	4	
Moderate	9	
Low	2	
Not categorized	1	
Certified and Accredited Systems - Total	744	95%
High	40	78%
Moderate	320	95%
Low	183	93%
Not categorized	201	100%
Tested Security Controls - Total	643	82%
High	37	73%
Moderate	263	78%
Low	142	72%
Not categorized	201	100%
Tested Contingency Plans - Total	497	63%
High	33	65%
Moderate	201	60%
Low	117	60%
Not categorized	146	72%
Total # of Systems not Categorized	202	
Incidents Reported Internally	44	
Incidents Reported to USCERT	38	
Incidents Reported to Law Enforcement	11	
Total Number of Employees	123,750	
Employees that received IT security awareness training	121,224	98%
Total Number of Employees w/significant IT security responsibilities	3,460	
Employees with significant responsibilities that received training	3,415	99%
Total Costs for providing IT security training	$2,280,126	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of the Treasury -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 51-70% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of the Treasury -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**406**	
Agency	394	
Contractor	12	
Systems requiring a Privacy Impact Assessment	**135**	
Agency	126	
Contractor	9	
Systems that have complete and current Privacy Impact Assessment	**123**	91%
Agency	115	
Contractor	8	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**307**	
Agency	298	
Contractor	9	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**253**	82%
Agency	251	
Contractor	2	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	Yes	
Agency annually reviews the use of persistent tracking.	No	

Department of the Treasury -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	Yes

Department of Veterans Affairs -- CIO Report

Total Number of Systems	**595**	
Agency Systems	**590**	
High	309	
Moderate	62	
Low	219	
Not categorized	0	
Contractor Systems	**5**	
High	2	
Moderate	3	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	593	100%
High	309	99%
Moderate	64	98%
Low	220	100%
Not categorized	0	0%
Tested Security Controls - Total	594	100%
High	310	100%
Moderate	64	98%
Low	220	100%
Not categorized	0	0%
Tested Contingency Plans - Total	215	36%
High	69	22%
Moderate	30	46%
Low	116	53%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	446	
Incidents Reported to USCERT	242	
Incidents Reported to Law Enforcement	91	
Total Number of Employees	236,317	
Employees that received IT security awareness training	234,216	99%
Total Number of Employees w/significant IT security responsibilities	877	
Employees with significant responsibilities that received training	877	100%
Total Costs for providing IT security training	$4,862,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	No	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of Veterans Affairs -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Rarely (0-50% of employees)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes

Department of Veterans Affairs -- Privacy Report

Systems that contain Federally-owned information in identifiable form	**172**	
Agency	172	
Contractor	0	
Systems requiring a Privacy Impact Assessment	**168**	
Agency	168	
Contractor	0	
Systems that have complete and current Privacy Impact Assessment	**167**	99%
Agency	167	
Contractor	0	
Systems of Records Notices- systems from which Federally-owned information is retrieved by name or unique identifier	**164**	
Agency	164	
Contractor	0	
Systems of Records Notices- systems for which a current SORN has been published in the Federal Register	**159**	97%
Agency	159	
Contractor	0	
The privacy official participates in all agency information privacy compliance activities.	Yes	
The privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and coments under Circular A-19.	Yes	
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	
The agency has a training program to ensure all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?	Yes	
The agency has a program for job-specific information privacy training for individuals involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Yes	
The agency has written processes or policies for all listed ascpects of Privacy Impact Assessments.	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Public-facing agency web sites have machine-readable privacy policies.	Yes	
Agency uses persistent tracking technology on any web site.	No	
Agency annually reviews the use of persistent tracking.	Yes	

Department of Veterans Affairs -- Privacy Report (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices?	Yes
Agency coordinates with OIG on privacy program oversight by providing to OIG the following materials:	
Compilation of agency's privacy and data protection policies and procedures	Yes
Summary of the agency's use of information in identifiable form	Yes
Verification of intent to comply with agency policies and procedures	Yes
Agency submits an annual report to Congress (OMB) detailing privacy activities, including activities under the Privacy Act and any violations that have occurred.	No

Appendix B: Reporting by Small and Independent Agencies

Background

Small and independent agencies manage a variety of Federal programs. Their responsibilities include issues concerning commerce and trade, energy and science, transportation, national security, and finance and culture. Approximately one half of the small and independent agencies perform regulatory or enforcement roles in the Federal Executive Branch. The remaining half is comprised largely of grant-making, advisory, and uniquely chartered organizations. A listing of small and independent agencies is included at the end of this appendix.

A "small agency" generally has less than six thousand employees; most have fewer than five hundred staff, and the smallest, called micro-agencies, have less than one hundred. Together these agencies employ about fifty thousand Federal workers and manage billions of taxpayer dollars.

Chief Information Officers (CIO) from the small and independent agencies participate in the Small Agency CIO Council which in turn is represented on the Federal CIO Council chaired by OMB. During fiscal year 2006, the Small Agency CIO Council worked with OMB to assist small agencies in complying with FISMA. On June 2, 2006, the Council hosted a joint CIO and IG briefing to discuss FISMA. OMB staff briefed the group on FISMA requirements and the latest security guidelines. On July 28, 2006, the Council held a special meeting to discuss privacy issues, followed by a meeting in September concentrating on privacy and encryption. The September meeting included demonstrations of products being used by small agencies to meet privacy guidelines.

FISMA Reporting Requirements and Results

FISMA applies to all agencies regardless of size. Except for micro-agencies, small and independent agencies follow the same reporting requirements as the large agencies.

This appendix contains an aggregated summary of reported performance metrics for small and independent agencies that submitted FISMA reports.

In fiscal year 2006, 53 small and independent agencies submitted FISMA reports, though only 50 of those reports contained data on security and privacy metrics. Of the 544 moderate-to-high impact systems reported:

- 37 percent of systems have been certified and accredited;
- 58 percent of systems have security controls tested and evaluated in the last year; and

- 39 percent of systems have tested contingency plans.

These statistics show significant decreases from the prior reporting period. OMB will work with the small and independent agencies to determine reasons for this trend. Through efforts such as the ISS LOB, we intend to make progress in closing these gaps.

Independent Assessments. 43 small and independent agencies conducted independent assessments of their systems in fiscal year 2005 (86 percent compared to 91 percent last year).

Implementation of NIST SP 800-53. 26 percent of small and independent agencies reported that they have fully implemented security controls in NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems."

Certification and Accreditation. 15 small and independent agencies (40 percent) have certified and accredited all of their systems. This represents a 43 percent increase over fiscal year 2005, when 40 percent of agencies reported success. Overall, 37 percent of high and moderate risk systems have certifications and accreditations.

Testing of Agency and Contractor Security Controls. 27 small and independent agencies (51 percent) reported that all agency and contractor systems' security controls were tested by FIPS-199 categorization in fiscal year 2005. Overall, 58 percent of high and moderate risk systems had tested security controls in fiscal year 2006.

Systems Categorized by FIPS-199. 40 small and independent agencies (80 percent) reported that all of their systems have been categorized by FIPS-199.

Incident Reporting to US-CERT. Although almost all small and independent agencies have policies requiring incident reporting to DHS, some fail to characterize abnormal system activity as reportable incidents. Seventeen small and independent agencies (32 percent) reported at least one abnormal system activity to the US-CERT in fiscal year 2005.

Security Awareness, Training and Education. Agencies provided various types of security awareness material for their employees, including self instructed web based programs, videos, e-mail alerts and employee newsletters.

For All Agency Employees Including Contractors. 15 small and independent agencies (28 percent) provided computer security awareness and training to 100 percent of their employees and contractors. 14 small and independent agencies (26 percent) provided computer security awareness and training to 90-99 percent of their employees and contractors. Seven small and independent agencies (13 percent) provided computer security awareness and training to 80-89 percent of

their employees and contractors. Overall, 91 percent of employees were trained in 2006.

For Employees with Significant Security Responsibilities. 21 small and independent agencies (40 percent) provided specialized computer security awareness and training to 100 percent of their employees and contractors with significant security responsibilities. 28 small and independent agencies (53 percent) provided specialized computer security awareness and training to at least 80 percent of their employees and contractors with significant security responsibilities. Overall, 78 percent of employees with significant security responsibilities were trained in 2006.

Tested Contingency Plans. 14 small and independent agencies reported that all of their high and moderate risk systems have tested contingency plans. Overall, 39 percent of high and moderate impact systems had tested contingency plans.

Small and Independent Agencies Submitting FISMA Reports in Fiscal Year 2005

1. African Development Foundation
2. American Battle Monuments Commission
3. Broadcasting Board of Governors
4. Christopher Columbus Foundation
5. Commodity Futures Trading Commission
6. Consumer Product Safety Commission
7. Corporation for National Community Services
8. Court Services & Offender Supervision Agency
9. Defense Nuclear Facilities Safety Board
10. Election Assistance Commission
11. Executive Office of the President
12. Equal Employment Opportunity Commission
13. Farm Credit Administration
14. Federal Communications Commission
15. Federal Deposit Insurance Corporation
16. Federal Election Commission
17. Federal Energy Regulatory Commission
18. Federal Housing Enterprise Oversight
19. Federal Housing Finance Board
20. Federal Maritime Commission
21. Federal Reserve System
22. Federal Retirement Thrift Investment Board
23. Federal Trade Commission
24. Import-Export Bank

25. Institute of Museum and Library Services
26. Inter-American Foundation
27. International Border and Water Commission
28. Japan-US Friendship Commission
29. Merit Systems Protection Board
30. Millennium Challenge Corporation
31. Morris K. Udall Foundation
32. National Archives and Records Administration
33. National Credit Union Administration
34. National Endowment for the Arts
35. National Endowment for the Humanities
36. National Gallery of Art
37. National Labor Relations Board
38. National Mediation Board
39. National Transportation Safety Board
40. Nuclear Waste Technical Review Board
41. Office of Government Ethics
42. Office of Special Counsel
43. Overseas Private Investment Corporation
44. Peace Corps
45. Pension Benefit Guaranty Corporation
46. Postal Rate Commission
47. Railroad Retirement Board
48. Securities and Exchange Commission
49. Selective Service System
50. Tennessee Valley Authority
51. US Access Board
52. US Holocaust Memorial Museum
53. US International Trade Commission
54. US Trade and Development Agency

Appendix C: Federal Government's IT Security Program

The Federal government's IT security program has evolved over the past two decades and applies to both unclassified and national security systems. The same management and evaluation requirements apply to both types of systems. However, while OMB and NIST set policies and guidance for federal non-national security systems, the interagency Committee on National Security Systems (CNSS) (established under National Security Directive 42) sets policies for federal national security systems.

The following cyber security governance structures have been designed for Federal National Security Systems, Federal non-National Security Systems and non-Federal systems.

Federal National Security Systems

National Security Systems are defined both in statute and regulation (see, e.g., 40 U.S.C. § 1452 as re-codified at 40 U.S.C. § 11103 and National Security Directive 42) as those systems that process classified information or unclassified systems that involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or equipment that is critical to the direct fulfillment of military or intelligence missions. Since the issuance of National Security Directive 42 in July 1990, the Secretary of Defense and the Director of the National Security Agency (NSA), respectively have served as the Federal government's Executive Agent and National Manager for National Security Telecommunications and Information Systems Security. The CNSS, chaired by the Assistant Secretary of Defense for Networks and Information Integration, serves as the US Government's policy-making body with authority to set Information Assurance (IA) standards and policies applicable to all National Security Systems. Additionally, the head of the US Intelligence Community, the Director of National Intelligence (formerly the Director of Central Intelligence), has statutory responsibility to protect intelligence sources and methods which have led to the promulgation of special cyber security policies for National Security Systems that process certain categories of intelligence.

Federal Non-National Security Systems

OMB is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security. NIST works collaboratively with OMB to develop standards and guidelines for Federal computer systems in order to achieve cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the NSA, where appropriate. Moreover, both NIST and OMB are

encouraged, and in some cases required, to coordinate with NSA "to assure, to the maximum extent feasible, that such standards and guidelines [for non-National Security Systems] are complementary with standards and guidelines developed for National Security Systems."

Non-Federal Systems

DHS works with and encourages the private sector, federal, state, tribal and local governments, academia, and the general public to protect the nation's information infrastructure. This role is authorized by the Homeland Security Act of 2002 and called for in the National Strategy to Secure Cyberspace. It is also reinforced more specifically in HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection.

HSPD-7 assigns the Secretary of DHS the responsibility of coordinating the nation's overall efforts in critical infrastructure protection across all sectors and tasks the Secretary to prepare a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives. This effort is now called the National Infrastructure Protection Plan (NIPP).

Statutory Requirements for Federal Non-National Security Systems

This appendix focuses on the Federal government's IT security program for unclassified systems. Applicable laws include:

- The Paperwork Reduction Act of 1995[12]. The Paperwork Reduction Act established a comprehensive information resources management framework and subsumed preexisting agency, NIST and OMB responsibilities under the Computer Security Act.

- The Clinger-Cohen Act of 1996[13]. The Clinger-Cohen Act linked OMB and agency security responsibilities to the information resources management, capital planning, and budget process and replaced most of the Computer Security Act.

- The Federal Information Security Management Act of 2002. FISMA reauthorized the provisions found in the Government Information Security Reform Act and amended the Paperwork Reduction Act of 1995. FISMA generally codifies OMB's security policies and continues the framework established in prior statute, while requiring annual agency program and system reviews, independent IG evaluations, annual agency reports to OMB, and an annual OMB report to

[12] 44 U.S.C. **§** 3501
[13] 40 U.S.C. § 1401(3)),

Congress. It also requires OMB to annually approve or disapprove agency programs. Additionally, FISMA emphasizes accountability for agency officials' security responsibilities. For example, the role of agency program officials in ensuring the systems supporting their operations and assets are appropriately secure is clearly defined.

Federal Agencies with Specific IT Security Responsibilities

Beyond securing their own systems, federal agencies with IT security responsibilities can be divided into two types – those with policy and guidance authorities and those with assistance, advice, and operational authorities. For the Federal government's unclassified IT security program, OMB and NIST issue policy and guidance. In the area of assistance, advice, and operations, the Preparedness Directorate of the Department of Homeland Security issues cyber alerts and warnings, provides government-wide assistance regarding intrusion detection and response, and partners with other organizations to protect our nation's critical cyber operations and assets.

1. Policy and Guidance Authorities

Office of Management and Budget - OMB is responsible for developing and overseeing the implementation of government-wide policies, principles, standards, as well as guidance for the Federal government's IT security program.

Within the statutory framework described earlier, OMB issues IT security policies (e.g., OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources"). OMB oversight and enforcement is achieved by reviewing and evaluating the following:

- IT budget submissions, such as the agency budget exhibit 53 and business case justifications for major IT investments;
- Annual agency and IG FISMA reports to OMB;
- Agency remediation efforts as demonstrated through their development, prioritization, and implementation of program and system level POA&Ms;
- Quarterly updates from agencies to OMB on their progress in remediating security weaknesses through completion of POA&Ms;
- Quarterly updates from agencies to OMB on their performance against key security measures;
- Quarterly assessment of agencies security status and progress through their E-Government Scorecard under the President's Management Agenda; and
- Annual OMB report to Congress.

OMB fulfills its policy and oversight role through the Office of E-Government, working with the Office of Information and Regulatory Affairs (OIRA).

National Institute of Standards and Technology - NIST is responsible for developing technical security standards and guidelines for unclassified Federal information systems. NIST publications are designed to:

- Promote, measure, and validate security in systems and services;
- Educate consumers; and
- Establish minimum security requirements for Federal systems.

NIST performs its statutory responsibilities through the Computer Security Division (CSD) of the IT Laboratory.

In accordance with FISMA, NIST must prepare an annual report describing activities completed in the previous year as well as detailing future actions to carry out FISMA responsibilities.

CSD's 2005 Annual Report can be found at: http://csrc.nist.gov/publications/nistir/7285/nistir-7285-CSD-2005-Annual-Report.pdf. The 2005 annual report highlights the publication of standards and guidelines which provide the foundation for strong information security programs for unclassified Federal information and information systems. In addition, the report discusses NIST's outreach program to promote the understanding of IT security vulnerabilities and corrective measures.

In fiscal year 2005, CSD was actively engaged in the following activities:

- Cryptographic Standards and Application;
- Security Testing and Metrics;
- Security Research/Emerging Technologies; and
- Security Management and Guidance.

Cryptographic Standards and Applications

Focus is on developing cryptographic methods for protecting the integrity, confidentiality, and authenticity of information resources; and addresses such technical areas as: secret and public key cryptographic techniques; advanced authentication

systems; cryptographic protocols and interfaces; public key certificate management; smart tokens; cryptographic key escrowing; and security architectures. Helps enable implementation of cryptographic services in applications and the national infrastructure. Current work and ongoing projects include:

- Cryptographic Standards Toolkit;
- Biometrics Standards Program and Security;
- E-Authentication;
- Infrastructure and Applications; and
- Public Voting System Standard Development.

Security Testing and Metrics

Focus is on working with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation; and addresses such areas as: development and maintenance of security metrics, security evaluation criteria and evaluation methodologies, tests and test methods; security-specific criteria for laboratory accreditation; guidance on the use of evaluated and tested products; research to address assurance methods and system-wide security and assessment methodologies; security protocol validation activities; and appropriate coordination with assessment-related activities of voluntary industry standards bodies and other assessment regimes. Current work and ongoing projects include:

- Automated Security Functional Testing and Test Suite Development; and
- Cryptographic Module Validation Program (CMVP);

Security Research/Emerging Technologies

Focus is on research necessary to understand and enhance the security utility of new technologies while also working to identify and mitigate vulnerabilities. This focus area addresses such technical areas as: advanced countermeasures such as intrusion detection, firewalls, and scanning tools; security test beds; vulnerability analysis/mitigation; access control; incident response; active code; and Internet security. Current projects include:

- Security Technical Implementation Guides and Checklists;
- Government Smart Care Program: International Standards Program;
- National Vulnerability Database;
- Authorization Management and Advanced Access Control Models;
- Reference Implementations for Automated Test Generation Tool-kit;
- Quantum Cryptography and Information Systems
- Internet Protocol Security (IPSec);

- Border Gateway Protocol;
- Domain Name System Security Extensions;
- Digital Handheld Device Forensics;
- Internet Protocol Version 6 (IPv6);
- Mobile Ad Hoc Network Security (MANET);
- Mobile Device Security;
- Dedicated Short Range Communications Security;
- Automated Software Testing Using Covering Arrays;
- Personal Identity Verification (PIV); and
- Wireless Security Standards.

Security Management and Guidance

Focus is on developing security management guidance, addressing such areas as: risk management, security program management, training and awareness, contingency planning, personnel security, administrative measures and procurement, and in facilitating security and the implementation of such guidance in Federal agencies via management and operation of the Computer Security Expert Assist Team. Current work and ongoing projects include:

- Automated Security Self-Evaluation Tool (ASSET);
- Anti-Spam Technologies;
- Federal Information Security Management Act (FISMA) Implementation Project;
- Minimum Security Requirements and Controls;
- Methods and Procedures for Assessing Security Controls;
- Organizational Accreditation Program;
- Security Practices and Policies;
- Revision of the Security Managers' Handbook;
- Guide to Performance Metrics for Information Security;
- Implementation of the Health Insurance and Accountability Act (HIPAA) Security Rule;
- Guide for Media Sanitation; and,
- Return on Investment for Security

Selected NIST Special Publications (Issued in Fiscal Year 2005)

- SP 800-79 Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations (July, 2005)

- SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification (April, 2005)
- SP 800-72 Guidelines on PDA Forensics (November, 2004)
- SP 800-70 Security Configuration Checklists Program for IT Products (May, 2005)
- SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (March, 2005)
- SP 800-65 Integrating Security into the Capital Planning and Investment Control Process (January, 2005)
- SP 800-58 Security Considerations for Voice Over IP systems (January, 2005)
- SP 800-53 Security Controls for Federal Information Systems (February, 2005)
- SP 800-52 Guidelines on the Selection and Use of Transport Layer Security (June, 2005)
- SP 800-38B Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode (May, 2005)

2. Assistance, Advice and Operations

Department of Homeland Security - US-CERT is a partnership between DHS and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating incident response activities.

US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

FISMA defines the following public sector responsibilities for US-CERT:

- Inform operators of agency information systems about current and potential information security threats and vulnerabilities. In fiscal year 2006, US-

CERT issued twenty-one Technical Cyber Security Alerts providing timely information about current security issues, vulnerabilities, and exploits. Agency officials were provided a description of the vulnerability, its impact, and the actions required to prevent exploitation of the weakness. Cyber Security Bulletins provide weekly summaries of security issues and new vulnerabilities. They also provide patches, workarounds, and other actions to help mitigate risk. Additionally, US-CERT published eleven non-technical Cyber Security Alerts which provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate computer users can take to protect themselves from attack.

- Compile and analyze information about incidents that threaten information security. US-CERT maintains a close working relationship with the major software manufacturers, Carnegie Mellon's Computer Emergency Response Team (CERT) and the law enforcement and intelligence communities. These parties work together to analyze malicious code and attribute attacks. In fiscal year 2006, agencies reported 5,146 incidents. US-CERT shared information regarding these incidents with Federal agencies, including members of the Government Forum of Incident Response and Security Teams (GFIRST). DHS created GFIRST in January 2004 as a community of Federal agency emergency computer response teams.

- Provide timely technical assistance regarding security incidents. The National Cyber Security Division (NCSD) maintains a 24x7 emergency hotline to advise agencies on preventing attacks and to respond to technical questions about compromised computers. In addition, NCSD uses the US-CERT Portal to communicate with members on a 24x7 basis about emerging cyber threats and vulnerabilities. The portal contains a set of tools to provide alert notification, secure e-mail messaging, live chat, document libraries, and a contact locator feature. The portal allows instant access to the US-CERT Operations team, the US-CERT Cyber Daily Briefing, and updated cyber event information.

- Consult with NIST and agencies operating national security systems regarding information security incidents. NCSD works closely with the intelligence community to understand emerging threat information. To do this, US-CERT conducts a daily conference call with the National Security Agency's National Security Incident Response Center, the Central Intelligence Agency's Intelligence Community Incident Response Center, DHS's Information Assurance Threat Analysis component and DOD's Joint Task Force-Global Network Operations to discuss classified cyber activity. In addition, NCSD has personnel on loan from the National Security Agency in its Law Enforcement

and Intelligence liaison section. Finally, NCSD maintains a close working relationship with the NIST Computer Security Division.