Office of Management and Budget

Fiscal Year 2008 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 2008, the Federal agencies spent $6.2 billion securing the government's total IT investment of approximately $68 billion for the fiscal year 2008 enacted level, equating to approximately 9.2 percent of the total IT portfolio. Funds spent on IT security are used for cross-cutting and system-specific security activities such as certification and accreditation (C&A) 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.

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. NIST performs its statutory responsibilities through the Computer Security Division of the Information Technology Laboratory.

NIST's report can be found at: http://csrc.nist.gov. The FY 2008 annual report highlights the continued development of standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Recognizing the potential benefits of more automation in technical security operations, NIST also hosted the Information Security Automation Program (ISAP), which formalizes and advances efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations. NIST continued to work closely with federal agencies to improve their understanding and implementation of FISMA to protect their information and information systems and publication of standards and guidelines which provide the foundation for strong information security programs at agencies. In addition, the report discusses NIST's outreach program to promote the understanding of IT security vulnerabilities and corrective measures.

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 privacy protections for personally identifiable information (PII), agencies are also required to report on performance metrics related to their privacy management programs. In addition to tracking the metrics for E-Government Act responsibilities, agencies are also required to report on additional metrics, including those associated with the Privacy Act (5 U.S.C. § 552a).

This report informs Congress and the public on the Federal government's performance against key security and privacy performance measures from fiscal year 2002 through fiscal year 2008. It also provides OMB's assessment of government-wide IT security strengths and weaknesses, outlines a plan of action to improve performance, and fulfills OMB's requirement under FISMA to submit an annual report to the Congress.

Data used within this report are based on fiscal year 2008 agency, IG, and privacy reports to OMB. Appendix A contains agency-specific security and privacy performance results for the 25 major Federal agencies. Appendix B provides a summary of FISMA and privacy performance results for small and independent agencies.

The national security and economic health of the United States depend on the security, stability, and integrity of our Nation's cyberspace, both in the public and private sectors. The President is confident that we can protect our nation's critical cyber infrastructure while at the same time adhering to the rule of law and safeguarding privacy rights and civil liberties. To that end, President Obama directed the National Security and Homeland Security Advisors to conduct an immediate review of the plan, programs, and activities underway throughout the government dedicated to cyber security. This 60-day interagency review will develop a strategic framework to ensure that U.S. Government cyber security initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector. We look forward to working with the Congress to ensure the successful protection of our nation's cyber security.

II. OMB Security and Privacy Reporting Guidance

OMB issues reporting guidance to agencies each year to acquire the information needed to oversee agency security programs and develop this report.[1] As in the past, OMB guidance for the fiscal year 2008 reporting period included quantitative and qualitative performance measures for the major provisions of FISMA. Key performance measures for C&A, controls testing, and contingency plan testing remain consistent in order to discern areas of improvement or those requiring improvement from year to year.

[1] See OMB Memorandum M-08-21 of July 14, 2008, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," at http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2008/m08-21.pdf

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

- 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 supporting 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 Plan of Action and Milestones (POA&M) process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. POA&Ms are the authoritative management tool used by an 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.

Privacy reporting guidance includes performance measures to assess agencies' handling of sensitive information, including PII. These performance measures reflect requirements from the E-Government Act, the Privacy Act, and related OMB memoranda. Additionally, agencies are required to provide the URL of the centrally located page on the agency web site listing working links to agency Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). For the 2007 annual report, OMB requested agencies provide copies of each of the four documents developed pursuant to OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." For 2008, OMB requested agencies submit the most up-to-date versions of the M-07-16 documents.

III. Government-wide Findings

A. Progress in Meeting Key Security Performance Measures

As illustrated in Table 1 below, the 25 major agencies of the Federal government continue to improve information security performance relative to C&A rates and testing of contingency plans for operational systems currently identified in their systems inventory. Testing of security controls decreased by two percent, from 95 percent in fiscal year 2007 to 93 percent in fiscal year 2008.

Table 1: Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2008

Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008
Certification and Accreditation	47%	62%	77%	85%	88%	92%	**96%**
Tested Contingency Plan	35%	48%	57%	61%	77%	86%	**92%**
Tested Security Controls	60%	64%	76%	72%	88%	95%	**93%**
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304	**10,679**

Certification and Accreditation

In fiscal year 2008, the percentage of certified and accredited systems rose to 96 percent from 92 percent in 2007. Twenty-three of the 25 major agencies report a C&A rate between 90 and 100 percent for operational systems, an increase of 16 percent over 2007. The Nuclear Regulatory Commission showed the most improvement in percentage increase in systems that have a C&A from 2007 to 2008, increasing from 17 percent to 59 percent of operational systems. The Department of Homeland Security also reported a considerable increase in C&A rates, improving from 84 percent to 94 percent. The Department of Defense reached and exceeded the 90 percent C&A rate in 2008, despite an increase in the number of systems by 158 in the inventory of operational systems for which a C&A is required. None of the 25 major agencies reported a sizable decrease in the number or percentage of systems with a C&A from 2007.

Testing of Contingency Plans and Security Controls

FISMA and OMB policy requires agencies to annually test both system contingency plans and security controls. In fiscal year 2008, agencies reported contingency plan testing and security controls testing for 92 percent and 93 percent of operational systems respectively. This shows an increase in contingency plan testing and a two percent overall decrease in security controls testing from the prior year. Three agencies reported significant increases in contingency plan testing, the Nuclear Regulatory Commission with an increase of 83 percent, the Department of Veterans Affairs with an increase of 57 percent, and the Department of Housing and Urban Development with an increase of 19 percent. Two agencies reported significant decreases in contingency plan testing: the Department of Education with a reduction of 23 percent and the Department of Agriculture with a 13 percent reduction.

Inventory of Systems

Twenty-four of 25 IGs reported their agencies' FISMA systems inventories were over 80 percent complete. Two agency IGs indicated they do not generally agree with the number of agency or contractor information systems identified in their inventories. The overall inventory of operational systems increased from 10,304 to 10,679 systems or by four percent from the prior year. The Departments of Defense and Energy increased their inventories, with Energy alone showing a 42 percent increase from 2007. The National Aeronautics and Space Administration and the Department of Treasury reported notable inventory decreases.

Quality of Certification and Accreditation Process

Ninety-two percent of agency IGs reported the overall quality of C&A processes to be "satisfactory" or better in fiscal year 2008, an increase from 76 percent in 2007.

Identifying Risk Impact Level

Table 2 below shows the distribution of risk impact levels[2] among agency and contractor systems and their respective C&A rates, contingency plan testing, and security controls testing.

Table 2: Fiscal Year 2008 FISMA System Inventory by Risk Impact Level

FIPS 199 Risk Impact Level	Number of Agency Systems	Number of Contractor Systems	Total Number of Systems	Percent certified and accredited	Percent with tested contingency plans	Percent with tested security controls
High	1,055	113	1,168	98%	90%	95%
Moderate	3,576	536	4,112	95%	92%	95%
Low	3,952	738	4,690	96%	90%	91%
Not Categorized	187	522	709	96%	96%	95%
Total	**8,770**	**1,909**	**10,679**	**96%**	**92%**	**93%**

Agencies reported a total of 10,679 systems categorized by a risk impact level of high, moderate, low, or not categorized. Of these systems, 8,770 are managed by Federal agencies, a decrease of 181 systems from 2007 to 2008. The number of systems reported as managed by a contractor or other organization on behalf of a Federal agency increased by 556 systems, from 1,353 to 1,909 from 2007 to 2008. The number of systems categorized as high risk fell in 2008 from 1,211 to 1,168 in 2007, while the number of systems categorized as moderate risk rose from 2007 to 2008, from 3,787 to 4,112. The number of systems not categorized by risk impact level rose from 613 in 2007 to 709 in 2008, 644 of which are classified systems within the Department of Energy categorized in accordance with federal policy for classified systems.

Employee Training in Systems Security

Agencies reported 89 percent of employees received security awareness training in 2008. Training for employees with significant information security responsibilities decreased significantly this year to 76 percent. Agencies reported spending over $95 million on all security training; more than $72 million of that amount is reported by three agencies: the Departments of Agriculture, Defense, and the Treasury.

Twenty-one of 25 IGs responded “Almost Always (96 to 100 percent of employees)” or “Mostly (81 to 95 percent of employees)” when asked if the agency has ensured security training and awareness for all employees, including contractors with significant IT security responsibilities. Eight agency IGs provided assessments for such training that conflicted with the levels reported

[2] In February 2004, NIST issued Federal Information Processing Standard (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems.” The standard establishes security categories for both information and information systems based on the potential impact on an organization should certain events occur that 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.

by the Chief Information Officer. Over two million employees, or 56 percent of those receiving security awareness training, were reported to have received the training via the Information Systems Security Line of Business (ISSLOB).

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. In 2008, eight IGs responded to this question with "Almost Always," decreasing from 12 in 2007 and 15 in 2006. From 2006 to 2008, the number of IGs responding to this question with "Almost Always" declined 47 percent.

Agency-wide Plan of Action and Milestones

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 responses in annual FISMA reports, 84 percent of agencies demonstrated they have an effective POA&M process in place for identifying and correcting weaknesses.

Configuration Management

The majority of major agencies reported they have adopted the Federal Desktop Core Configuration (FDCC) as their agency policy and are making progress configuring existing desktops and laptops. Many agencies have also incorporated FDCC requirements into their procurement activities. Only ten agencies reported that they followed common NIST configuration standards "almost always" or "mostly."

NIST has developed tools, now available from vendors that allow agencies to test their laptops and desktops to determine that the configurations are in compliance with FDCC. A pilot program under GSA is currently testing statistical samples of workstations at major agencies to help agencies keep track of their compliance.

B. Progress in Meeting Key Privacy Performance Measures

As discussed in the sections that follow, the fiscal year 2008 agency FISMA reports indicate improvements in privacy performance measures.

Table 3: Status and Progress of Key Privacy Performance Measures

	FY 2006	**FY 2007**	**FY 2008**
Number of systems containing information in identifiable form	2,870	3,259	3,505
Number of systems requiring a PIA	1,321	1,826	2,002
Number of systems with a PIA	1,113	1,525	1,850
Percentage of systems with a PIA	**84%**	**84%**	**92%**
Number of systems requiring a SORN	1,874	2,607	2,373

Number of systems with a SORN	1,555	2,169	2,205
Percentage of systems with a SORN	**83%**	**83%**	**93%**

Privacy Program Oversight

In 2008, 23 out of 25 senior agency officials for privacy reported participation in all three privacy responsibility categories, including privacy compliance activities, assessments of information technology, and evaluating legislative, regulatory, and other agency policy proposals for privacy. All agencies reported having policies in place to ensure that all personnel with access to Federal data are familiar with information privacy requirements, and 21 out of 25 agencies reported having targeted, job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 100 percent of applicable systems to have publicly posted PIAs. In 2008, 92 percent of applicable systems within the 25 major agencies had publicly posted PIAs, an increase over 84 percent in 2007. The increase occurred as the number of systems requiring a PIA also increased.

Quality of Privacy Impact Assessment Process

FISMA reporting guidance asks agency IGs to rate the quality of each agency's PIA process. In 2008, 24 out of 25 agencies received an assessment of its PIA process as "Satisfactory" or better, and one agency received a "Failing" rating. The ratings represent an improvement since 2007. In 2007, 19 of 23 agencies evaluated by their IGs received an assessment of their PIA process as "Satisfactory" or better. Three agencies were reported as having "Poor" PIA processes, and one as having a "Failing" PIA process.

System of Records Notices

The Federal goal is for 100 percent of applicable information systems with Privacy Act records to have developed, published, and maintained SORNs. In 2008, 93 percent of information systems government-wide with Privacy Act records have published current SORNs. The percentage represents an overall increase from 2007, reflecting the combined effect of an increase in information systems with SORNs and a decrease in the number of information systems required to be covered by a SORN.

Privacy-Related Policies and Plans

On May 22, 2007, OMB issued Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* setting forth four new privacy directives for agencies to:

- Develop and implement a breach notification plan;
- Implement a plan to eliminate unnecessary collection and use of SSNs in agency programs;
- Implement a plan to review and reduce unnecessary holdings of PII; and

- Develop policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

OMB requested up-to-date plans and policies associated with the requirements. Since the issuance of M-07-16, agencies demonstrated progress in establishing breach notification plans, providing a better foundation for responding to breaches of PII. Most agencies were able to provide formal, comprehensive breach notification polices. Agencies also included model documents, such as sample breach notification letters, along with the plans for rapid response to a breach.

Despite varying levels of detail and comprehensiveness across agencies, the submitted plans for reducing unnecessary Social Security Numbers (SSNs) and PII, as well as establishing related rules of behavior, generally demonstrate agency officials have been sensitized to the privacy risks associated with SSN and PII holdings. The efforts will require on-going oversight through the capital planning process, Paperwork Reduction Act reviews, Executive Order 12866 regulatory reviews, and other oversight mechanisms. In order to facilitate agency SSN reduction efforts, Executive Order 13478, "Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers" removed a requirement for agencies to use SSNs as individuals' unique identifiers.

IV. Summary of Government-wide IG Security and Privacy 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.

Table 4 shows a summary of the IG results and assessments for the 25 major Federal agencies for fiscal year 2008. Text in bold in Table 4 indicates a change from prior year reporting, with a "+" indicating a performance improvement and a "-" indicating a performance downgrade. The results of these findings were previously discussed in Section III of this report, "Government-wide Findings."

Table 4: Results of IG Assessments for Fiscal Year 2008 FISMA annual report

Agency	Effective POA&M ?	Quality of Certification and Accreditation Process	Completeness of System Inventory	Quality of Privacy Impact Assessment Process
Agency for International Development	Yes	Excellent	96-100%	**Excellent +**
Department of Agriculture	No	Poor	**81-95% +**	**Satisfactory +**
Department of Commerce	Yes	**Satisfactory** +	96-100%	Good
Department of Defense	No	Failing	0	Failing
Department of Education	Yes	Satisfactory	96-100%	**Excellent +**
Department of Energy	Yes	Satisfactory	96-100%	Satisfactory
Environmental Protection Agency	Yes	**Good** +	96-100%	**Excellent +**
General Services Administration	Yes	Satisfactory	96-100%	Satisfactory
Department of Health and Human Services	Yes	**Satisfactory -**	**81-95% -**	**Good -**
Department of Homeland Security	Yes	**Good +**	96-100%	Good
Department of Housing and Urban Development	Yes	Satisfactory	96-100%	**Satisfactory -**
Department of the Interior	No	**Satisfactory +**	96-100%	**Excellent +**
Department of Justice	Yes	**Good -**	96-100%	Excellent
Department of Labor	Yes	Satisfactory	96-100%	Good
National Aeronautics and Space Administration	**Yes**	**Excellent +**	96-100%	Good
National Science Foundation	Yes	Good	96-100%	Excellent
Nuclear Regulatory Commission	Yes	**Satisfactory +**	**96-100% +**	Excellent
Office of Personnel Management	Yes	**Satisfactory -**	96-100%	**Excellent +**
Small Business Administration	Yes	Satisfactory	96-100%	Satisfactory
Smithsonian Institution	Yes	Satisfactory	**96-100% +**	**Satisfactory -**
Social Security Administration	Yes	**Good -**	96-100%	**Excellent +**
Department of State	**Yes**	**Good +**	96-100 %	**Good +**
Department of Transportation	**No**	Satisfactory	96-100%	**Satisfactory -**
Department of the Treasury	Yes	Satisfactory	**96-100% +**	Satisfactory
Department of Veterans Affairs	**Yes**	**Satisfactory +**	**96-100% +**	**Satisfactory +**

V. OMB Assessment of Agency Incident Handling Programs

FISMA requires each agency to document and implement procedures for detecting, reporting, and responding to security incidents. Agencies must also notify and consult with the United States Computer Emergency Readiness Team (US-CERT).[3] The act also requires OMB oversight of the US-CERT and NIST to issue incident detection and handling guidelines.

Agencies overwhelmingly report having in place procedures for reporting incidents both internally and externally. These procedures include both reporting to US CERT and, where appropriate, to law enforcement. Twenty-two of 25 major agencies report logging and monitoring activities involving access to and modification of sensitive or critical information. All 25 major agencies reported having incident handling and response programs, including reporting capabilities.

VI. Plan of Action to Improve Performance

Under the new Administration, OMB will continue to work with agencies, IGs, CIOs, Senior Agency Officials for Privacy, GAO, and the Congress to strengthen the Federal government's IT security and privacy programs. As part of those activities, OMB will:

1. Review Agency Business Cases

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

2. Evaluate Reported Security Metrics

We will be reviewing the security metrics provided by agencies in their quarterly and annual reports for FISMA compliance. The increased reported compliance by the agencies, which is supported by the IG's reports, indicates that it could be time to modify the metrics to improve the assurance of security. One goal for new metrics would be to move beyond periodic compliance reporting to more continuous monitoring of security.

3. Review Current Cyber-security Activities

The President has requested a 60-day review of all Cyber-security activities within the Federal Government. OMB will be participating in this review.

[3] Contact information for US-CERT: www.uscert.gov

Website Addresses	http://www.us-cert.gov	https://www.us-cert.gov	
Email Addresses	soc@us-cert.gov	us-cert@dhs.sgov.gov (SIPR)	us-cert@dhs.ic.gov (JWICS)

VII. Conclusion

Over the past year, most of the 25 major Federal agencies made incremental progress in closing the Federal government's IT security performance gaps against established performance criteria.

Moving forward, agencies should continue to focus management attention on:

- Achieving 100 percent C&A levels for all operational systems;
- Properly identifying and providing oversight of contractor systems; and
- Maintaining PIAs and SORNs for 100 percent of applicable systems

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

Appendix A: Fiscal Year 2008 Government-wide Summary

Table of Contents

FY 2008 Government-wide Summary -- CIO Reports

Total Number of systems	**10,677**	
Agency systems	**8,768**	
High	1055	
Moderate	3576	
Low	3950	
Not categorized	187	
Contractor systems	**1,909**	
High	113	
Moderate	536	
Low	738	
Not categorized	522	
Certified and Accredited Systems - Total	10,257	**96%**
High	1143	98%
Moderate	3924	95%
Low	4507	96%
Not categorized	683	96%
Tested Security Controls - Total	9,970	93%
High	1110	95%
Moderate	3902	95%
Low	4287	91%
Not categorized	671	95%
Tested Contingency Plans - Total	9,770	92%
High	1056	90%
Moderate	3797	92%
Low	4236	90%
Not categorized	681	96%
Total # of Systems not Categorized	709	7%
Total Number of Employees	4,162,322	
Employees that received IT security awareness training	3,723,241	89%
Employees that received IT security awareness training using ISSLOB	2,085,880	
Total Number of Employees with significant IT security responsibilities	147263	
Employees with significant responsibilities that received training	111680	76%
Total Costs for providing IT security training	$95,424,039	

The agency explains policies regarding peer-to-peer file sharing in training	Yes	23	agencies
	No	2	agencies
There is an agency-wide security configuration policy	Yes	25	agencies
	No	0	agencies
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	1	agencies
	Sometimes (51-70% of the time)	1	agencies
	Frequently (71-80% of the time)	4	agencies
	Mostly (81-95% of the time)	7	agencies
	Almost Always (96-100% of the time)	12	agencies
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	19	agencies
	No	6	agencies

-This page left blank intentionally-

FY 2008 Government-wide Summary -- IG Reports

Quality of agency C&A process	Excellent	2 agencies	
	Good	6 agencies	
	Satisfactory	15 agencies	
	Poor	1 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	Rarely (0-50% of the time)		2 agencies
	Sometimes (51-70% of the time)		3 agencies
	Frequently (71-80% of the time)		7 agencies
	Mostly (81-95% of the time)		3 agencies
	Almost Always (96-100% of the time)		8 agencies
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Approximately 0-50% complete		1 agencies
	Approximately 51-70% complete		0 agencies
	Approximately 71-80% complete		0 agencies
	Approximately 81-95% complete		2 agencies
	Approximately 96-100% complete		22 agencies
The OIG generally agrees with the CIO on the number of agency owned systems	Yes	23 agencies	
	No	2 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	23 agencies	
	No	2 agencies	
The agency inventory is maintained and updated at least annually	Yes	24 agencies	
	No	1 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	Rarely (0-50% of the time)		2 agencies
	Sometimes (51-70% of the time)		2 agencies
	Frequently (71-80% of the time)		1 agencies
	Mostly (81-95% of the time)		6 agencies
	Almost Always (96-100% of the time)		14 agencies
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time)		3 agencies
	Sometimes (51-70% of the time)		0 agencies
	Frequently (71-80% of the time)		3 agencies
	Mostly (81-95% of the time)		5 agencies
	Almost Always (96-100% of the time)		14 agencies
Effective POA&M process? 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.	Yes	21 agencies	
	No	4 agencies	
There is an agency wide security configuration policy	Yes	23 agencies	
	No	2 agencies	

FY 2008 Government-wide Summary -- IG Reports (continued)

The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes	19	agencies
	No	6	agencies
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes	23	agencies
	No	2	agencies
The agency follows defined procedures for reporting to the USCERT	Yes	21	agencies
	No	4	agencies
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Rarely (0-50% of employees)	2	agencies
	Sometimes (51-70% of employees)	1	agencies
	Frequently (71-80% of employees)	1	agencies
	Mostly (81-95% of employees)	9	agencies
	Almost Always (96-100% of employees)	12	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	20	agencies
	No	5	agencies
The agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards are	Excellent	9	agencies
	Good	6	agencies
	Satisfactory	9	agencies
	Poor	0	agencies
	Failing	1	agencies
The agency has completed system e-authentication risk assessments	Yes	13	agencies
	No	12	agencies

FY 2008 Government-wide Summary -- Privacy Reports

Systems that contain Federal information in identifiable form	**3,505**		
Agency	3,076		
Contractor	429		
Systems requiring a Privacy Impact Assessment under the E-Gov Act	**2,002**		
Agency	1,757		
Contractor	245		
Systems covered by an existing Privacy Impact Assessment	**1,850**	92%	
Agency	1,649		
Contractor	201		
Systems for which a system or records notice (SORN) is required under the Privacy Act	**2,373**		
Agency	2,078		
Contractor	295		
Systems for which a current SORN has been published in the Federal Register	**2,205**	93%	
Agency	1,923		
Contractor	282		
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 comments under Circular A-19.	Yes	23	agencies
	No	2	agencies
The privacy official participates in assessing the impact of technology on the privacy of personal information.	Yes	24	agencies
	No	1	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	25	agencies
	No	0	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
The agency has written processes or policies for all listed aspects 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	24	agencies
	No	0	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	15	agencies
	No	10	agencies

FY 2008 Government-wide Summary -- Privacy Reports (continued)

Agency has current documentation demonstrating review of compliance with information privacy laws, regulations and policies.	Yes	24 agencies
	No	1 agencies
Agency can provide documentation demonstrating corrective action planned, in progress, or completed to remedy identified compliance deficiencies.	Yes	24 agencies
	No	1 agencies
Agency uses technologies that allow for continuous auditing of compliance with stated privacy policies and practices.	Yes	16 agencies
	No	9 agencies
Agency coordinates with OIG on privacy program oversight	Yes	24 agencies
	No	1 agencies

US Agency for International Development -- CIO Report

Total Number of Systems	29	
Agency Systems	18	
High	0	
Moderate	17	
Low	1	
Not categorized	0	
Contractor Systems	11	
High	0	
Moderate	6	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	29	100%
High	0	0%
Moderate	23	100%
Low	6	100%
Not categorized	0	0%
Tested Security Controls - Total	29	100%
High	0	0%
Moderate	23	100%
Low	6	100%
Not categorized	0	0%
Tested Contingency Plans - Total	29	100%
High	0	0%
Moderate	23	100%
Low	6	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	8,826	
Employees that received IT security awareness training	8,826	100%
Employees that received IT security awareness training using ISSLOB	8,826	
Total Number of Employees w/significant IT security responsibilities	203	
Employees with significant responsibilities that received training	192	95%
Total Costs for providing IT security training	$45,711	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an identification 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

US Agency for International Development -- Privacy Report

Systems that contain Federal information in identifiable form	4	
Agency	3	
Contractor	1	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	4	
Agency	3	
Contractor	1	
Systems covered by an existing Privacy Impact Assessment	4	100%
Agency	3	
Contractor	1	
Systems for which a system or records notice (SORN) is required under the Privacy Act	3	
Agency	2	
Contractor	1	
Systems for which a current SORN has been published in the Federal Register	3	100%
Agency	2	
Contractor	1	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Agriculture -- CIO Report

Total Number of Systems	245	
Agency Systems	239	
High	18	
Moderate	162	
Low	59	
Not categorized	0	
Contractor Systems	6	
High	0	
Moderate	6	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	222	91%
High	18	100%
Moderate	149	89%
Low	55	93%
Not categorized	0	0%
Tested Security Controls - Total	224	91%
High	18	100%
Moderate	162	96%
Low	44	75%
Not categorized	0	0%
Tested Contingency Plans - Total	208	85%
High	17	94%
Moderate	143	85%
Low	48	81%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	129,642	
Employees that received IT security awareness training	123,177	95%
Employees that received IT security awareness training using ISSLOB	117,018	
Total Number of Employees w/significant IT security responsibilities	1,980	
Employees with significant responsibilities that received training	1,933	98%
Total Costs for providing IT security training	$11,596,250	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
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	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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	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	Almost Always (96-100%)
Effective POA&M process	No
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	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	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	No
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Agriculture -- Privacy Report

Systems that contain Federal information in identifiable form	100	
Agency	96	
Contractor	4	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	100	
Agency	96	
Contractor	4	
Systems covered by an existing Privacy Impact Assessment	100	100%
Agency	96	
Contractor	4	
Systems for which a system or records notice (SORN) is required under the Privacy Act	88	
Agency	84	
Contractor	4	
Systems for which a current SORN has been published in the Federal Register	85	97%
Agency	81	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Commerce -- CIO Report

Total Number of Systems	312	
Agency Systems	292	
High	22	
Moderate	206	
Low	54	
Not categorized	10	
Contractor Systems	20	
High	4	
Moderate	13	
Low	3	
Not categorized	0	
Certified and Accredited Systems - Total	299	96%
High	23	88%
Moderate	210	96%
Low	56	98%
Not categorized	10	100%
Tested Security Controls - Total	304	97%
High	26	100%
Moderate	211	96%
Low	57	100%
Not categorized	10	100%
Tested Contingency Plans - Total	307	98%
High	25	96%
Moderate	216	99%
Low	56	98%
Not categorized	10	100%
Total # of Systems not Categorized	10	
Total Number of Employees (including contractors)	51,624	
Employees that received IT security awareness training	51,377	100%
Employees that received IT security awareness training using ISSLOB	12,330	
Total Number of Employees w/significant IT security responsibilities	863	
Employees with significant responsibilities that received training	782	91%
Total Costs for providing IT security training	$1,491,589	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
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)	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 identification of interfaces (including those not under control of the agency)	The inventory is 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 time)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Commerce -- Privacy Report

Systems that contain Federal information in identifiable form	49	
Agency	49	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	49	
Agency	49	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	49	100%
Agency	49	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	48	
Agency	48	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	48	100%
Agency	48	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	Yes	
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	Yes	

-This page left blank intentionally-

Department of Defense -- CIO Report

Total Number of Systems	4279	
Agency Systems	4182	
High	265	
Moderate	1059	
Low	2809	
Not categorized	49	
Contractor Systems	97	
High	1	
Moderate	26	
Low	64	
Not categorized	6	
Certified and Accredited Systems - Total	4074	95%
High	259	97%
Moderate	1034	95%
Low	2727	95%
Not categorized	54	98%
Tested Security Controls - Total	3903	91%
High	234	88%
Moderate	1004	93%
Low	2613	91%
Not categorized	52	95%
Tested Contingency Plans - Total	3836	90%
High	241	91%
Moderate	989	91%
Low	2554	89%
Not categorized	52	95%
Total # of Systems not Categorized	55	
Total Number of Employees (including contractors)	2,414,169	
Employees that received IT security awareness training	2,091,176	87%
Employees that received IT security awareness training using ISSLOB	1,264,715	
Total Number of Employees w/significant IT security responsibilities	90,163	
Employees with significant responsibilities that received training	58,700	65%
Total Costs for providing IT security training	$31,687,887	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 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
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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Failing
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Defense -- Privacy Report

Systems that contain Federal information in identifiable form	709	
Agency	689	
Contractor	20	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	200	
Agency	194	
Contractor	6	
Systems covered by an existing Privacy Impact Assessment	181	91%
Agency	176	
Contractor	5	
Systems for which a system or records notice (SORN) is required under the Privacy Act	471	
Agency	463	
Contractor	8	
Systems for which a current SORN has been published in the Federal Register	350	74%
Agency	344	
Contractor	6	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	No	
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	Yes	

-This page left blank intentionally-

Department of Education -- CIO Report

Total Number of Systems	145	
Agency Systems	68	
High	1	
Moderate	18	
Low	49	
Not categorized	0	
Contractor Systems	77	
High	2	
Moderate	31	
Low	44	
Not categorized	0	
Certified and Accredited Systems - Total	125	86%
High	3	100%
Moderate	39	80%
Low	83	89%
Not categorized	0	0%
Tested Security Controls - Total	127	88%
High	3	100%
Moderate	41	84%
Low	83	89%
Not categorized	0	0%
Tested Contingency Plans - Total	94	65%
High	1	33%
Moderate	37	76%
Low	56	60%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	13,509	
Employees that received IT security awareness training	13,465	100%
Employees that received IT security awareness training using ISSLOB	13,465	
Total Number of Employees w/significant IT security responsibilities	2,096	
Employees with significant responsibilities that received training	2,090	100%
Total Costs for providing IT security training	$283,211	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
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	Almost Always (96-100% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 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
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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Education -- Privacy Report

Systems that contain Federal information in identifiable form	99	
Agency	60	
Contractor	39	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	34	
Agency	21	
Contractor	13	
Systems covered by an existing Privacy Impact Assessment	32	94%
Agency	19	
Contractor	13	
Systems for which a system or records notice (SORN) is required under the Privacy Act	96	
Agency	56	
Contractor	40	
Systems for which a current SORN has been published in the Federal Register	94	98%
Agency	55	
Contractor	39	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies.	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking.	No	
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	Yes	

-This page left blank intentionally-

Department of Energy -- CIO Report

Total Number of Systems	1323	
Agency Systems	281	
High	8	
Moderate	103	
Low	42	
Not categorized	128	
Contractor Systems	1042	
High	7	
Moderate	95	
Low	424	
Not categorized	516	
Certified and Accredited Systems - Total	1269	96%
High	14	93%
Moderate	175	88%
Low	461	99%
Not categorized	619	96%
Tested Security Controls - Total	1181	89%
High	14	93%
Moderate	170	86%
Low	388	83%
Not categorized	609	95%
Tested Contingency Plans - Total	1245	94%
High	15	100%
Moderate	154	78%
Low	457	98%
Not categorized	619	96%
Total # of Systems not Categorized	644	
Total Number of Employees (including contractors)	146,043	
Employees that received IT security awareness training	143,844	98%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	5,985	
Employees with significant responsibilities that received training	5,743	96%
Total Costs for providing IT security training	$5,185,982	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Energy -- 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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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	Frequently (71-80% of the time)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Energy -- Privacy Report

Systems that contain Federal information in identifiable form	153	
Agency	72	
Contractor	81	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	81	
Agency	42	
Contractor	39	
Systems covered by an existing Privacy Impact Assessment	79	98%
Agency	40	
Contractor	39	
Systems for which a system or records notice (SORN) is required under the Privacy Act	23	
Agency	16	
Contractor	7	
Systems for which a current SORN has been published in the Federal Register	23	100%
Agency	16	
Contractor	7	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

Environmental Protection Agency -- CIO Report

Total Number of Systems	171	
Agency Systems	155	
High	1	
Moderate	116	
Low	38	
Not categorized	0	
Contractor Systems	16	
High	0	
Moderate	11	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	171	100%
High	1	100%
Moderate	127	100%
Low	43	100%
Not categorized	0	0%
Tested Security Controls - Total	171	100%
High	1	100%
Moderate	127	100%
Low	43	100%
Not categorized	0	0%
Tested Contingency Plans - Total	171	100%
High	1	100%
Moderate	127	100%
Low	43	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	21,329	
Employees that received IT security awareness training	21,329	100%
Employees that received IT security awareness training using ISSLOB	21,329	
Total Number of Employees w/significant IT security responsibilities	584	
Employees with significant responsibilities that received training	553	95%
Total Costs for providing IT security training	$538,402	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
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	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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%)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Environmental Protection Agency -- Privacy Report

Systems that contain Federal information in identifiable form	36	
Agency	34	
Contractor	2	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	36	
Agency	34	
Contractor	2	
Systems covered by an existing Privacy Impact Assessment	36	100%
Agency	34	
Contractor	2	
Systems for which a system or records notice (SORN) is required under the Privacy Act	32	
Agency	30	
Contractor	2	
Systems for which a current SORN has been published in the Federal Register	32	100%
Agency	30	
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 comments 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	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	No	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

General Services Administration -- CIO Report

Total Number of Systems	85	
Agency Systems	40	
High	0	
Moderate	31	
Low	9	
Not categorized	0	
Contractor Systems	45	
High	1	
Moderate	36	
Low	8	
Not categorized	0	
Certified and Accredited Systems - Total	85	100%
High	1	100%
Moderate	67	100%
Low	17	100%
Not categorized	0	0%
Tested Security Controls - Total	85	100%
High	1	100%
Moderate	67	100%
Low	17	100%
Not categorized	0	0%
Tested Contingency Plans - Total	85	100%
High	1	100%
Moderate	67	100%
Low	17	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	14,957	
Employees that received IT security awareness training	14,957	100%
Employees that received IT security awareness training using ISSLOB	14,957	
Total Number of Employees w/significant IT security responsibilities	146	
Employees with significant responsibilities that received training	141	97%
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 applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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%)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100%)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

General Services Administration -- Privacy Report

Systems that contain Federal information in identifiable form	40	
Agency	26	
Contractor	14	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	16	
Agency	6	
Contractor	10	
Systems covered by an existing Privacy Impact Assessment	16	100%
Agency	6	
Contractor	10	
Systems for which a system or records notice (SORN) is required under the Privacy Act	40	
Agency	27	
Contractor	13	
Systems for which a current SORN has been published in the Federal Register	40	100%
Agency	27	
Contractor	13	
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 comments 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	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Health and Human Services -- CIO Report

Total Number of Systems	162	
Agency Systems	129	
High	34	
Moderate	77	
Low	18	
Not categorized	0	
Contractor Systems	33	
High	12	
Moderate	16	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	162	100%
High	46	100%
Moderate	93	100%
Low	23	100%
Not categorized	0	0%
Tested Security Controls - Total	162	100%
High	46	100%
Moderate	93	100%
Low	23	100%
Not categorized	0	0%
Tested Contingency Plans - Total	162	100%
High	46	100%
Moderate	93	100%
Low	23	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	99,708	
Employees that received IT security awareness training	98,511	99%
Employees that received IT security awareness training using ISSLOB	4,236	
Total Number of Employees w/significant IT security responsibilities	5,930	
Employees with significant responsibilities that received training	5,268	89%
Total Costs for providing IT security training	$2,649,761	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 81-95% 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	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
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 the time)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	Yes
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Health and Human Services -- Privacy Report

Systems that contain Federal information in identifiable form	94	
Agency	78	
Contractor	16	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	94	
Agency	78	
Contractor	16	
Systems covered by an existing Privacy Impact Assessment	94	100%
Agency	78	
Contractor	16	
Systems for which a system or records notice (SORN) is required under the Privacy Act	72	
Agency	60	
Contractor	12	
Systems for which a current SORN has been published in the Federal Register	69	96%
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Homeland Security -- CIO Report

Total Number of Systems	591	
Agency Systems	376	
High	121	
Moderate	210	
Low	45	
Not categorized	0	
Contractor Systems	215	
High	55	
Moderate	129	
Low	31	
Not categorized	0	
Certified and Accredited Systems - Total	560	95%
High	174	99%
Moderate	314	93%
Low	72	95%
Not categorized	0	0%
Tested Security Controls - Total	584	99%
High	176	100%
Moderate	333	98%
Low	75	99%
Not categorized	0	0%
Tested Contingency Plans - Total	552	93%
High	154	88%
Moderate	322	95%
Low	76	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	231,425	
Employees that received IT security awareness training	222,694	96%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	2,100	
Employees with significant responsibilities that received training	1,967	94%
Total Costs for providing IT security training	$2,313,823	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
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	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 identification of interfaces (including those not under control of the agency)	The inventory is 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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Homeland Security -- Privacy Report

Systems that contain Federal information in identifiable form	288	
Agency	151	
Contractor	137	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	169	
Agency	86	
Contractor	83	
Systems covered by an existing Privacy Impact Assessment	81	48%
Agency	37	
Contractor	44	
Systems for which a system or records notice (SORN) is required under the Privacy Act	265	
Agency	137	
Contractor	128	
Systems for which a current SORN has been published in the Federal Register	238	90%
Agency	119	
Contractor	119	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Housing and Urban Development -- CIO Report

Total Number of Systems	86	
Agency Systems	77	
High	3	
Moderate	67	
Low	7	
Not categorized	0	
Contractor Systems	9	
High	0	
Moderate	6	
Low	3	
Not categorized	0	
Certified and Accredited Systems - Total	86	100%
High	3	100%
Moderate	73	100%
Low	10	100%
Not categorized	0	0%
Tested Security Controls - Total	78	91%
High	3	100%
Moderate	65	89%
Low	10	100%
Not categorized	0	0%
Tested Contingency Plans - Total	86	100%
High	3	100%
Moderate	73	100%
Low	10	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	10,283	
Employees that received IT security awareness training	9,976	97%
Employees that received IT security awareness training using ISSLOB	9,677	
Total Number of Employees w/significant IT security responsibilities	186	
Employees with significant responsibilities that received training	100	54%
Total Costs for providing IT security training	$0	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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%)
Effective POA&M process	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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Housing and Urban Development -- Privacy Report

Systems that contain Federal information in identifiable form	79	
Agency	72	
Contractor	7	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	27	
Agency	26	
Contractor	1	
Systems covered by an existing Privacy Impact Assessment	27	100%
Agency	26	
Contractor	1	
Systems for which a system or records notice (SORN) is required under the Privacy Act	50	
Agency	49	
Contractor	1	
Systems for which a current SORN has been published in the Federal Register	49	98%
Agency	48	
Contractor	1	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

Department of Interior -- CIO Report

Total Number of Systems	177	
Agency Systems	158	
High	5	
Moderate	127	
Low	26	
Not categorized	0	
Contractor Systems	19	
High	4	
Moderate	11	
Low	4	
Not categorized	0	
Certified and Accredited Systems - Total	168	95%
High	9	100%
Moderate	130	94%
Low	29	97%
Not categorized	0	0%
Tested Security Controls - Total	173	98%
High	9	100%
Moderate	134	97%
Low	30	100%
Not categorized	0	0%
Tested Contingency Plans - Total	157	89%
High	9	100%
Moderate	121	88%
Low	27	90%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	71,162	
Employees that received IT security awareness training	69,780	98%
Employees that received IT security awareness training using ISSLOB	69,773	
Total Number of Employees w/significant IT security responsibilities	3,271	
Employees with significant responsibilities that received training	3,032	93%
Total Costs for providing IT security training	$630,166	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Interior -- 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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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	Rarely (0-50% of the time)
Effective POA&M process	No
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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Interior -- Privacy Report

Systems that contain Federal information in identifiable form	224	
Agency	220	
Contractor	4	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	179	
Agency	175	
Contractor	4	
Systems covered by an existing Privacy Impact Assessment	179	100%
Agency	174	
Contractor	5	
Systems for which a system or records notice (SORN) is required under the Privacy Act	97	
Agency	93	
Contractor	4	
Systems for which a current SORN has been published in the Federal Register	97	100%
Agency	93	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Justice -- CIO Report

Total Number of Systems	254	
Agency Systems	239	
High	90	
Moderate	102	
Low	47	
Not categorized	0	
Contractor Systems	15	
High	2	
Moderate	9	
Low	4	
Not categorized	0	
Certified and Accredited Systems - Total	254	100%
High	92	100%
Moderate	111	100%
Low	51	100%
Not categorized	0	0%
Tested Security Controls - Total	254	100%
High	92	100%
Moderate	111	100%
Low	51	100%
Not categorized	0	0%
Tested Contingency Plans - Total	254	100%
High	92	100%
Moderate	111	100%
Low	51	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	128,944	
Employees that received IT security awareness training	125,962	98%
Employees that received IT security awareness training using ISSLOB	42,827	
Total Number of Employees w/significant IT security responsibilities	2,193	
Employees with significant responsibilities that received training	2,141	98%
Total Costs for providing IT security training	$2,106,065	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	N/A
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Justice -- Privacy Report

Systems that contain Federal information in identifiable form	191	
Agency	183	
Contractor	8	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	70	
Agency	66	
Contractor	4	
Systems covered by an existing Privacy Impact Assessment	65	93%
Agency	62	
Contractor	3	
Systems for which a system or records notice (SORN) is required under the Privacy Act	156	
Agency	148	
Contractor	8	
Systems for which a current SORN has been published in the Federal Register	156	100%
Agency	148	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Labor -- CIO Report

Total Number of Systems	72	
Agency Systems	62	
High	0	
Moderate	62	
Low	0	
Not categorized	0	
Contractor Systems	10	
High	0	
Moderate	10	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	72	100%
High	0	0%
Moderate	72	100%
Low	0	0%
Not categorized	0	0%
Tested Security Controls - Total	72	100%
High	0	0%
Moderate	72	100%
Low	0	0%
Not categorized	0	0%
Tested Contingency Plans - Total	72	100%
High	0	0%
Moderate	72	100%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	17,122	
Employees that received IT security awareness training	16,443	96%
Employees that received IT security awareness training using ISSLOB	15,785	
Total Number of Employees w/significant IT security responsibilities	722	
Employees with significant responsibilities that received training	682	94%
Total Costs for providing IT security training	$576,605	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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 identification of interfaces (including those not under control of the agency)	The inventory is 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
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	No
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of Labor -- Privacy Report

Systems that contain Federal information in identifiable form	55	
Agency	44	
Contractor	11	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	39	
Agency	28	
Contractor	11	
Systems covered by an existing Privacy Impact Assessment	39	100%
Agency	28	
Contractor	11	
Systems for which a system or records notice (SORN) is required under the Privacy Act	39	
Agency	31	
Contractor	8	
Systems for which a current SORN has been published in the Federal Register	37	95%
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

National Aeronautics and Space Administration -- CIO Report

Total Number of Systems	634	
Agency Systems	604	
High	65	
Moderate	305	
Low	234	
Not categorized	0	
Contractor Systems	30	
High	3	
Moderate	18	
Low	9	
Not categorized	0	
Certified and Accredited Systems - Total	617	97%
High	66	97%
Moderate	313	97%
Low	238	98%
Not categorized	0	0%
Tested Security Controls - Total	586	92%
High	64	94%
Moderate	305	94%
Low	217	89%
Not categorized	0	0%
Tested Contingency Plans - Total	579	91%
High	66	97%
Moderate	301	93%
Low	212	87%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	69,893	
Employees that received IT security awareness training	65,226	93%
Employees that received IT security awareness training using ISSLOB	65,226	
Total Number of Employees w/significant IT security responsibilities	3,888	
Employees with significant responsibilities that received training	3,879	100%
Total Costs for providing IT security training	$736,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Frequently (71-80% of the time)	
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	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	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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	Almost Always (96-100% of the time)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

National Aeronautics and Space Administration -- Privacy Report

Systems that contain Federal information in identifiable form	35	
Agency	17	
Contractor	18	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	11	
Agency	5	
Contractor	6	
Systems covered by an existing Privacy Impact Assessment	11	100%
Agency	5	
Contractor	6	
Systems for which a system or records notice (SORN) is required under the Privacy Act	11	
Agency	5	
Contractor	6	
Systems for which a current SORN has been published in the Federal Register	11	100%
Agency	5	
Contractor	6	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

National Science Foundation -- CIO Report

Total Number of Systems	20	
Agency Systems	17	
High	0	
Moderate	12	
Low	5	
Not categorized	0	
Contractor Systems	3	
High	1	
Moderate	2	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	20	100%
High	1	100%
Moderate	14	100%
Low	5	100%
Not categorized	0	0%
Tested Security Controls - Total	20	100%
High	1	100%
Moderate	14	100%
Low	5	100%
Not categorized	0	0%
Tested Contingency Plans - Total	20	100%
High	1	100%
Moderate	14	100%
Low	5	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	6,137	
Employees that received IT security awareness training	5,977	97%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	81	
Employees with significant responsibilities that received training	81	100%
Total Costs for providing IT security training	$28,410	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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 identification of interfaces (including those not under control of the agency)	The inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

National Science Foundation -- Privacy Report

Systems that contain Federal information in identifiable form	5	
Agency	5	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	5	
Agency	5	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	5	100%
Agency	5	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	5	
Agency	5	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	5	100%
Agency	5	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

Nuclear Regulatory Commission -- CIO Report

Total Number of Systems	39	
Agency Systems	28	
High	11	
Moderate	17	
Low	0	
Not categorized	0	
Contractor Systems	11	
High	1	
Moderate	9	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	23	59%
High	5	42%
Moderate	17	65%
Low	1	100%
Not categorized	0	0%
Tested Security Controls - Total	38	97%
High	12	100%
Moderate	25	96%
Low	1	100%
Not categorized	0	0%
Tested Contingency Plans - Total	39	100%
High	12	100%
Moderate	26	100%
Low	1	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	4,540	
Employees that received IT security awareness training	4,378	96%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	550	
Employees with significant responsibilities that received training	60	11%
Total Costs for providing IT security training	$100,931	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
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	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 identification of interfaces (including those not under control of the agency)	Inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Nuclear Regulatory Commission -- Privacy Report

Systems that contain Federal information in identifiable form	62	
Agency	50	
Contractor	12	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	23	
Agency	15	
Contractor	8	
Systems covered by an existing Privacy Impact Assessment	23	100%
Agency	15	
Contractor	8	
Systems for which a system or records notice (SORN) is required under the Privacy Act	40	
Agency	30	
Contractor	10	
Systems for which a current SORN has been published in the Federal Register	40	100%
Agency	30	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

Office of Personnel Management -- CIO Report

Total Number of Systems	40	
Agency Systems	30	
High	5	
Moderate	24	
Low	1	
Not categorized	0	
Contractor Systems	10	
High	2	
Moderate	8	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	39	98%
High	7	100%
Moderate	31	97%
Low	1	100%
Not categorized	0	0%
Tested Security Controls - Total	40	100%
High	7	100%
Moderate	32	100%
Low	1	100%
Not categorized	0	0%
Tested Contingency Plans - Total	39	98%
High	7	100%
Moderate	31	97%
Low	1	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	12,114	
Employees that received IT security awareness training	11,649	96%
Employees that received IT security awareness training using ISSLOB	11,183	
Total Number of Employees w/significant IT security responsibilities	108	
Employees with significant responsibilities that received training	108	100%
Total Costs for providing IT security training	$49,163	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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 identification of interfaces (including those not under control of the agency)	The inventory is 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	Mostly (81-95% of the time)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Office of Personnel Management-- Privacy Report

Systems that contain Federal information in identifiable form	32	
Agency	22	
Contractor	10	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	24	
Agency	16	
Contractor	8	
Systems covered by an existing Privacy Impact Assessment	24	100%
Agency	16	
Contractor	8	
Systems for which a system or records notice (SORN) is required under the Privacy Act	29	
Agency	19	
Contractor	10	
Systems for which a current SORN has been published in the Federal Register	28	97%
Agency	19	
Contractor	9	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Small Business Administration -- CIO Report

Total Number of Systems	93	
Agency Systems	83	
High	4	
Moderate	14	
Low	65	
Not categorized	0	
Contractor Systems	10	
High	2	
Moderate	8	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	92	99%
High	5	83%
Moderate	22	100%
Low	65	100%
Not categorized	0	0%
Tested Security Controls - Total	92	99%
High	6	100%
Moderate	21	95%
Low	65	100%
Not categorized	0	0%
Tested Contingency Plans - Total	92	99%
High	6	100%
Moderate	21	95%
Low	65	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	4,425	
Employees that received IT security awareness training	3,949	89%
Employees that received IT security awareness training using ISSLOB	3,949	
Total Number of Employees w/significant IT security responsibilities	75	
Employees with significant responsibilities that received training	75	100%
Total Costs for providing IT security training	$75,360	
The agency explains policies regarding peer-to-peer file sharing in training	No	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

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	Frequently 71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Small Business Administration -- Privacy Report

Systems that contain Federal information in identifiable form	27	
Agency	24	
Contractor	3	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	27	
Agency	24	
Contractor	3	
Systems covered by an existing Privacy Impact Assessment	27	100%
Agency	24	
Contractor	3	
Systems for which a system or records notice (SORN) is required under the Privacy Act	27	
Agency	24	
Contractor	3	
Systems for which a current SORN has been published in the Federal Register	27	100%
Agency	24	
Contractor	3	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	No	
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	Yes	

-This page left blank intentionally-

Smithsonian Institution -- CIO Report

Total Number of Systems	14	
Agency Systems	13	
High	0	
Moderate	7	
Low	6	
Not categorized	0	
Contractor Systems	1	
High	0	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	14	100%
High	0	0%
Moderate	8	100%
Low	6	100%
Not categorized	0	0%
Tested Security Controls - Total	14	100%
High	0	0%
Moderate	8	100%
Low	6	100%
Not categorized	0	0%
Tested Contingency Plans - Total	14	100%
High	0	0%
Moderate	8	100%
Low	6	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	9,693	
Employees that received IT security awareness training	9,501	98%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	94	
Employees with significant responsibilities that received training	49	52%
Total Costs for providing IT security training	$42,536	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
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 identification of interfaces (including those not under control of the agency)	Inventory is 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	Frequently (71-80% of the time)
Effective POA&M process	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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

* Effective POA&M determined by Agency Head.

Smithsonian Institution -- Privacy Report

Systems that contain Federal information in identifiable form	10	
Agency	9	
Contractor	1	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	10	
Agency	9	
Contractor	1	
Systems covered by an existing Privacy Impact Assessment	10	100%
Agency	9	
Contractor	1	
Systems for which a system or records notice (SORN) is required under the Privacy Act	0	
Agency	0	
Contractor	0	
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 comments under Circular A-19	No	
The privacy official participates in assessing the impact of technology on the privacy of personal information	No	
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	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	No	

-This page left blank intentionally-

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	
Total Number of Employees (including contractors)	83,238	
Employees that received IT security awareness training	61,140	73%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	356	
Employees with significant responsibilities that received training	356	100%
Total Costs for providing IT security training	$1,389,784	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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	n/a
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Excellent
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Social Security Administration -- Privacy Report

Systems that contain Federal information in identifiable form	20	
Agency	20	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	17	
Agency	17	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	17	100%
Agency	17	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	20	
Agency	20	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	20	100%
Agency	20	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of State -- CIO Report

Total Number of Systems	356	
Agency Systems	238	
High	37	
Moderate	121	
Low	80	
Not categorized	0	
Contractor Systems	118	
High	0	
Moderate	23	
Low	95	
Not categorized	0	
Certified and Accredited Systems - Total	356	100%
High	37	100%
Moderate	144	100%
Low	175	100%
Not categorized	0	0%
Tested Security Controls - Total	352	99%
High	37	100%
Moderate	140	97%
Low	175	100%
Not categorized	0	0%
Tested Contingency Plans - Total	356	100%
High	37	100%
Moderate	144	100%
Low	175	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	95,000	
Employees that received IT security awareness training	95,000	100%
Employees that received IT security awareness training using ISSLOB	95,000	
Total Number of Employees w/significant IT security responsibilities	2,742	
Employees with significant responsibilities that received training	2,742	100%
Total Costs for providing IT security training	$2,700,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Almost Always (96-100% of the time)	
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	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	The inventory is 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
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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Good
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	Yes

Department of State -- Privacy Report

Systems that contain Federal information in identifiable form	92	
Agency	92	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	59	
Agency	59	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	59	100%
Agency	59	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	82	
Agency	82	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	81	99%
Agency	81	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Transportation -- CIO Report

Total Number of Systems	405	
Agency Systems	353	
High	25	
Moderate	235	
Low	93	
Not categorized	0	
Contractor Systems	52	
High	3	
Moderate	33	
Low	16	
Not categorized	0	
Certified and Accredited Systems - Total	387	96%
High	26	93%
Moderate	258	96%
Low	103	94%
Not categorized	0	0%
Tested Security Controls - Total	363	90%
High	21	75%
Moderate	242	90%
Low	100	92%
Not categorized	0	0%
Tested Contingency Plans - Total	353	87%
High	25	89%
Moderate	233	87%
Low	95	87%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	73,132	
Employees that received IT security awareness training	60,794	83%
Employees that received IT security awareness training using ISSLOB	60,794	
Total Number of Employees w/significant IT security responsibilities	523	
Employees with significant responsibilities that received training	473	90%
Total Costs for providing IT security training	$202,000	
The agency explains policies regarding peer-to-peer file sharing in training	No	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Rarely (0-50% of the time)	
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	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 identification of interfaces (including those not under control of the agency)	The inventory is 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	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
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	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 the time)
The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training	No
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Transportation -- Privacy Report

Systems that contain Federal information in identifiable form	139	
Agency	110	
Contractor	29	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	74	
Agency	60	
Contractor	14	
Systems covered by an existing Privacy Impact Assessment	53	72%
Agency	43	
Contractor	10	
Systems for which a system or records notice (SORN) is required under the Privacy Act	97	
Agency	78	
Contractor	19	
Systems for which a current SORN has been published in the Federal Register	97	100%
Agency	78	
Contractor	19	
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 comments 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	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	Yes	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Treasury -- CIO Report

Total Number of Systems	509	
Agency Systems	484	
High	33	
Moderate	352	
Low	99	
Not categorized	0	
Contractor Systems	25	
High	6	
Moderate	17	
Low	2	
Not categorized	0	
Certified and Accredited Systems - Total	495	97%
High	39	100%
Moderate	356	96%
Low	100	99%
Not categorized	0	0%
Tested Security Controls - Total	506	99%
High	39	100%
Moderate	366	99%
Low	101	100%
Not categorized	0	0%
Tested Contingency Plans - Total	496	97%
High	37	95%
Moderate	358	97%
Low	101	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	124,929	
Employees that received IT security awareness training	123,610	99%
Employees that received IT security awareness training using ISSLOB	0	
Total Number of Employees w/significant IT security responsibilities	6,308	
Employees with significant responsibilities that received training	6,221	99%
Total Costs for providing IT security training	$29,369,723	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Mostly (81-95% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Treasury -- 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 identification of interfaces (including those not under control of the agency)	Inventory is 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	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	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Treasury -- Privacy Report

Systems that contain Federal information in identifiable form	388	
Agency	376	
Contractor	12	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	336	
Agency	325	
Contractor	11	
Systems covered by an existing Privacy Impact Assessment	330	98%
Agency	319	
Contractor	11	
Systems for which a system or records notice (SORN) is required under the Privacy Act	297	
Agency	286	
Contractor	11	
Systems for which a current SORN has been published in the Federal Register	297	100%
Agency	286	
Contractor	11	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Department of Veterans Affairs -- CIO Report

Total Number of Systems	618	
Agency Systems	584	
High	307	
Moderate	124	
Low	153	
Not categorized	0	
Contractor Systems	34	
High	7	
Moderate	12	
Low	15	
Not categorized	0	
Certified and Accredited Systems - Total	618	100%
High	314	100%
Moderate	136	100%
Low	168	100%
Not categorized	0	0%
Tested Security Controls - Total	592	96%
High	300	96%
Moderate	128	94%
Low	164	98%
Not categorized	0	0%
Tested Contingency Plans - Total	504	82%
High	260	83%
Moderate	105	77%
Low	139	83%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Total Number of Employees (including contractors)	320,478	
Employees that received IT security awareness training	270,500	84%
Employees that received IT security awareness training using ISSLOB	254,750	
Total Number of Employees w/significant IT security responsibilities	16,116	
Employees with significant responsibilities that received training	14,312	89%
Total Costs for providing IT security training	$1,474,680	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency applies common security configuration established by NIST to application information systems	Sometimes (51-70% of the time)	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Veterans Affairs -- 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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an identification of interfaces (including those not under control of the agency)	Inventory is 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	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	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process	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
Quality of the agency's PIA process, as discussed in Section D 11.4 (SAOP template), including adherence to existing policy, guidance and standards	Satisfactory
Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with NIST Special Publication 800-63, "Electronic Authentication Guidelines"?	No

Department of Veteran Affairs -- Privacy Report

Systems that contain Federal information in identifiable form	574	
Agency	574	
Contractor	0	
Systems requiring a Privacy Impact Assessment under the E-Gov Act	318	
Agency	318	
Contractor	0	
Systems covered by an existing Privacy Impact Assessment	309	97%
Agency	309	
Contractor	0	
Systems for which a system or records notice (SORN) is required under the Privacy Act	285	
Agency	285	
Contractor	0	
Systems for which a current SORN has been published in the Federal Register	285	100%
Agency	285	
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 comments 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 aspects of Privacy Impact Assessments	Yes	
The agency has written process for determining continued compliance with stated web privacy policies	Yes	
Agency uses persistent tracking technology on any web site	No	
Agency annually reviews the use of persistent tracking	Yes	
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	Yes	

-This page left blank intentionally-

Appendix B: Fiscal Year 2008 FISMA 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 "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 sixty-six thousand Federal workers and manage billions of taxpayer dollars.

FISMA Reporting Requirements for Small and Independent Agencies

FISMA applies to all agencies regardless of size. Except for micro-agencies, small and independent agencies follow the same annual reporting requirements as the large agencies. The fiscal year 2008 FISMA reporting guidance eliminated the requirement for all small, independent, and micro agencies to submit quarterly FISMA reports, unless specifically asked to do so by OMB on a case-by-case basis.

Summary of Fiscal Year 2007 Small and Independent Agencies Reporting Results

In FY 2008, 60 small, independent, and micro agencies submitted FISMA reports. This appendix contains an aggregated summary of reported performance measures for those agencies that submitted reports with usable data. Since the data reporting requirements for small agencies differ from those for micro agencies, the results are separated accordingly and summarized in the tables below:

Small Agencies FISMA Performance	**FY 2007**	**FY 2008**	**Performance Increase/Decrease**
Number of Agencies Reporting Data	41	39	Decrease
Systems with Certification and Accreditation	71%	78%	Increase
Systems with Tested Contingency Plan	70%	66%	Decrease
Systems with Tested Security Controls	79%	78%	Decrease
Total Systems Reported	407	411	Increase
Conducted Independent Assessment	90%	92%	Increase
Agency Implemented NIST SP 800-53	46%	64%	Increase
Agency Categorized all Systems by FIPS-199	80%	74%	Decrease

Small Agencies FISMA Performance	FY 2007	FY 2008	Performance Increase/Decrease
Employees and Contractors who received Security Awareness Training	89%	88%	Decrease
Employees with Significant Security Responsibilities who received Training	85%	91%	Increase
Applicable Systems with Privacy Impact Assessments	77%	80%	Increase
Applicable Systems with System of Records Notice	90%	91%	Increase

* This number likely reflects incorrect reporting.

Micro Agencies FISMA status	FY 2007	FY 2008	Performance Increase/Decrease
Number of agencies reporting data	15	21	Increase
Systems with Certification and Accreditation	65%	80%	Increase
Systems with Tested Security Controls	75%	83%	Increase
Total Systems Reported	40	59	Increase
Agency Conducted Independent Assessment	60%	62%	Increase
Employees and Contractors who received Security Awareness Training	84%	97%	Increase

The majority of small and independent agencies submitted annual FISMA reports for fiscal year 2008, listed below:

1. African Development Foundation
2. American Battle Monuments Commission
3. Armed Forces Retirement Home
4. Barry Goldwater Scholarship and Excellence in Education Foundation
5. Broadcasting Board of Governors
6. Chemical Safety Board
7. Christopher Columbus Foundation
8. Commodity Futures Trading Commission
9. Consumer Product Safety
10. Corporation for National Community Services
11. Court Services & Offender Supervision Agency
12. Defense Nuclear Facilities Safety Board
13. Denali Commission
14. Equal Employment Opportunity Commission
15. Executive Office of the President
16. Export Import Bank of the United States
17. Farm Credit Administration
18. Federal Communications Commission
19. Federal Deposit Insurance Corp
20. Federal Election Commission
21. Federal Energy Regulation Commission
22. Federal Housing Enterprise Oversight (now the Federal Housing Finance Agency (FHFA)
23. Federal Housing Finance Board
24. Federal Maritime Commission
25. Federal Reserve System
26. Federal Retirement Thrift Investment Board
27. Federal Trade Commission
28. Institute of Museum and Library Services
29. Inter-American Foundation
30. James Madison Memorial Fellowship Foundation
31. Japan-U.S. Friendship Commission

32. Merit Systems Protection Board
33. Millennium Challenge Corp
34. Morris K. Udall Foundation
35. National Archives and Records Administration
36. National Credit Union Administration
37. National Endowment for the Arts
38. National Endowment for the Humanities
39. National Gallery of Art
40. National Labor Relations Board
41. National Mediation Board
42. National Transportation Safety Board
43. Nuclear Waste Technical Review Board
44. Occupational Safety and Health Review Commission
45. Office of Government Ethics
46. Office of Navajo and Hopi Indian Relocation
47. Office of Special Counsel
48. Overseas Private Investment Corporation
49. Peace Corps
50. Pension Benefit Guaranty Corp
51. Postal Regulatory Commission
52. Railroad Retirement Board
53. Securities and Exchange Commission
54. Selective Service System
55. Tennessee Valley Authority
56. U.S. Commission of Fine Arts
57. U.S. Commission on Civil Rights
58. U.S. Election Assistance Commission
59. U.S. Holocaust Memorial Museum
60. U.S. International Boundary and Water Commission
61. U.S. International Trade Commission
62. U.S. Trade and Development Agency