Office of Management and Budget

FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002

March 1, 2006

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). Its goals 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 is a significant undertaking. In FY 2005, the Federal agencies spent $5.0 billion securing the government's total information technology investment of approximately $62 billion or about eight percent of the total information technology portfolio.

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 information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, 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 the Act.

This report informs Congress and the public of the Federal government's security performance, and fulfills OMB's requirement under FISMA to submit an annual report to the Congress. It provides OMB's assessment of government-wide information technology security strengths and weaknesses and a plan of action to improve performance. It also examines agency status against key security performance measures from FY 2002 through FY 2005.

Data used within this report is based on FY 2005 agency and IG reports to OMB. Appendix A contains statistical summaries of security performance at 25 large agencies. Appendix B provides a summary of small and independent agency compliance with FISMA. Finally, Appendix C of the report summarizes the roles and responsibilities within the Federal government's information technology security program.

II. OMB Security Reporting Guidance

To acquire information needed to oversee agency security programs and develop this report, each year OMB issues reporting guidance to the agencies.[1] As in the past, this year's guidance included quantitative performance measures for the major provisions of FISMA to help identify agency status and progress. Many of this year's performance measures are identical to past

[1] See OMB Memorandum M-05-15 of June 13, 2005. "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" at www.whitehouse.gov/omb/memoranda/2005.html

years' guidance. Consequently, areas of improvement, as well as areas requiring additional management attention are easily discernable.

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

- Inventory of Systems. FISMA continues the Paperwork Reduction Act of 1995 (44 U.S.C. §101 note) requirement for agencies to develop and maintain an inventory of major information systems (including national security systems) operated by or under the control of the agency. The inventory must be used to support monitoring, testing and evaluation of information security controls.

- Contractor Operations and Facilities. FISMA requires Federal agencies to provide information security for the information and information systems *that support the operations and assets of the agency*, including those provided or managed by another agency, contractor, or other source. When this condition is met, agencies must provide evaluations extending beyond traditional agency boundaries.

- Implementation of security configurations. FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. In addition, agencies must explain the degree to which they implement and enforce security configurations.

- Plan of Action and Milestones. FISMA requires agencies to develop a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.[2]

III. Government-wide Findings - Progress in Meeting Key Security Performance Measures

The FY 2005 agency FISMA reports reveal progress in meeting several key security performance measures:

- Certifying and accrediting systems. The number of certified and accredited systems rose from 77% to 85%. At the same time, agencies reported a 19% increase in the total number of IT systems – from 8,623 in FY 2004 to 10,289 in FY 2005. Several agencies have made outstanding progress in FY 2005. The Department of Defense moved from 58% to 82% of systems certified and accredited and the Department of Veterans Affairs improved from 14% to 100%.

[2] In OMB's FISMA guidance, this process is called a security plan of action and milestones (POA&M). POA&Ms are the authoritative management tool used by the agency (including the IG) to detail specific program and system-level security weaknesses, remediation needs, the resources required to implement the plan, and scheduled completion dates.

- Assigning a risk impact level.[3] For the first time, agencies reported in FY 2005 on the total number of systems assigned a risk impact level (high, moderate or low). Agencies reported a total of 10,289 systems. Of these, 9,184 systems were managed by Federal agencies and 1,105 were managed by a contractor or other organization on behalf of a Federal agency. Overall, 1,646 agency systems were categorized as high impact, 2,497 as moderate impact, and 4,456 as low impact. Of the 1,105 contractor systems, 295 were categorized as high impact, 252 as medium impact, and 168 as low impact. As of October 2005, agencies reported that 585 agency systems and 390 contractor systems had not yet been assigned a risk impact level. It is encouraging to note that the overall certification and accreditation percentage for high impact systems is 88%, higher than the overall certification and accreditation average, showing that agencies are prioritizing their systems and working first to secure the systems presenting the highest risk impact level.

- Quality of certification and accreditation. Inspectors General reported the overall quality of the certification and accreditation processes at agencies increased with 17 of 25 agencies having a process in place rated as "satisfactory" or better, up from 15 agencies last year.

- Quality of agency corrective plans of action and milestone process (POA&M). Based on OMB analysis, IG reports show that 19 of 25 agencies have effective POA&M processes. This is an increase from 18 agencies last year. In addition, IGs report that in FY 2005, 21 agencies had a system inventory that was over 80% complete, and 25 agencies had an agency-wide security configuration policy in place. IG results for these measures are detailed below, in the section entitled "*Government-wide IG Evaluation Results*."

[3] In February 2004, NIST issued Federal Information Processing Standard 199 "Standards for Security Categorization of Federal Information and Information Systems". The standard establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. The process used by agencies to determine FIPS 199 categories is similar to the December 2003 Homeland Security Presidential Directive (HSPD) -7 requirement to identify, prioritize and protect critical infrastructure. Those cyber assets identified as "nationally critical" under HSPD-7 would be categorized as high impact under FIPS 199.

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

Table 1: Security Status and Progress from FY 2002 to FY 2005[4]				
Percentage of Systems with a:	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**
Certification and Accreditation	47%	62%	77%	**85%**
Tested Contingency Plan	35%	48%	57%	**61%**
Tested Security Control	60%	64%	76%	**72%**

While several improvements have been made in FY 2005, agency reports reveal areas requiring strategic and continued management attention over the coming year, including:

- 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. Most (18 of 24) agency IGs categorized the extent of agency's oversight as "mostly" (5 agencies)"almost always" (10 agencies) or "frequently" (3 agencies); however, several (6 of 24) agency IGs rate the extent of agency oversight as "rarely" (3 agencies) or "sometimes" (3 agencies). One agency IG did not evaluate this element. Through quarterly reporting mechanisms, OMB now requires agencies to track key performance metrics for FISMA compliance for contractor systems that are part of the system inventory.

- Testing of security controls. FISMA and OMB policy requires agencies to test system security controls annually. In FY 2005, agencies tested these controls on 72% of all systems, down from 76% in FY 2004.[5] However, it is apparent from the data that agencies are properly prioritizing security control testing, since the percentage of high impact systems tested was appreciably higher, at 83%. OMB continues to track this metric quarterly, by risk impact level, and uses this metric as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Incident Reporting. Although agencies participated in development of the incident handling concept of operations last year, DHS continues to find sporadic reporting by

[4] Total number of systems reported: FY2002=7957; FY2003=7998; FY2004=8623; FY2005=10289. The system count changes as agencies refine their system inventory and acquire, consolidate, or retire systems.
Total number of systems with a certification and accreditation: FY2002=3772; FY2003=4969; FY2004=6607; FY2005=8735
Total number of systems with a tested contingency plan: FY2002=2768; FY2003=3835; FY2004=4886; FY2005=6230
Total number of systems with tested security controls: FY2002=4751; FY2003=5143; FY2004=6515; FY2005=7425

[5] The total number of systems increased from 8623 in FY 2004 to 10289 in FY 2005.

some agencies and unusually low levels of reporting by others. Less than full reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event, e.g., the widespread propagation of an Internet worm.

- Agency-wide plans of action and milestones (POA&Ms). OMB policy requires agencies to prepare POA&Ms for all programs and systems where a security weakness has been found, and asks agency IGs to evaluate this process. Based on OMB analysis, IG reports show that 19 agencies have effective POA&M processes, however reports from 6 other agencies reveal weaknesses which indicate ineffective processes. OMB encourages CIOs and IGs to work together to remediate these process weaknesses, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Quality of certification and accreditation process. One IG rated the agency certification and accreditation process as "excellent." Four IGs rated the agency certification and accreditation process as "good", and 12 rated it as "satisfactory." While none of the IGs rated the certification and accreditation process as failing, 8 rated the process as "poor." OMB encourages agency CIOs and IGs to work together to improve the quality of the agency's C&A process, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

In addition to the government-wide statistics above, Appendix A provides detail on individual Federal agencies' performance against key security performance measures. The tables within the appendix contain information from the agencies' FY 2005 FISMA reports.

IV. Government-wide IG 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.

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

Table 2: Agency Inspector Generals were asked several questions to evaluate whether the agency maintains an effective plan of action and milestones process to remediate IT security weaknesses. To arrive at "Effective" as shown in this table, OMB considers a set of IG responses, including how weaknesses are incorporated in the POA&M, how they are prioritized, and how the status of weaknesses is tracked and reported.

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

Table 3: Agency Inspector Generals were asked to evaluate the quality of agency certification and accreditation processes. They were given response choices including: excellent, good, satisfactory, poor and failing.

Agency	Evaluation
Agency for International Development	Good
Department of Agriculture	Poor
Department of Commerce	Poor
Department of Defense	Poor
Department of Education	Satisfactory
Department of Energy	Poor
Environmental Protection Agency	Good
General Services Administration	Satisfactory
Department of Health and Human Services	Satisfactory
Department of Homeland Security	Poor
Department of Housing and Urban Development	Satisfactory
Department of the Interior	Poor
Department of Justice	Good
Department of Labor	Satisfactory
National Aeronautics and Space Administration	Satisfactory
National Science Foundation	Good
Nuclear Regulatory Commission	Poor
Office of Personnel Management	Satisfactory
Small Business Administration	Satisfactory
Smithsonian Institution	Poor
Social Security Administration	Excellent
Department of State	Satisfactory
Department of Transportation	Satisfactory
Department of the Treasury	Satisfactory
Department of Veterans Affairs	Satisfactory
Total "Excellent":	1
Total "Good":	4
Total "Satisfactory":	12
Total "Poor":	8
Total "Failing":	0

Table 4: Agency Inspector Generals were asked to evaluate the extent to which an agency system inventory has been developed. They were given several response choices including: Approximately 0-50% complete, 51-50% complete, 71-80% complete, 81-95% complete, and 96-100% complete.

Agency	Evaluation
Agency for International Development	96-100%
Department of Agriculture	0-50%
Department of Commerce	96-100%
Department of Defense	0-50%
Department of Education	96-100%
Department of Energy	51-70%
Environmental Protection Agency	96-100%
General Services Administration	96-100%
Department of Health and Human Services	81-95%
Department of Homeland Security	96-100%
Department of Housing and Urban Development	81-95%
Department of the Interior	81-95%
Department of Justice	81-95%
Department of Labor	96-100%
National Aeronautics and Space Administration	96-100%
National Science Foundation	96-100%
Nuclear Regulatory Commission	51-70%
Office of Personnel Management	96-100%
Small Business Administration	96-100%
Smithsonian Institution	81-95%
Social Security Administration	96-100%
Department of State	81-95%
Department of Transportation	96-100%
Department of the Treasury	81-95%
Department of Veterans Affairs	81-95%
Total “Approximately 96-100% complete”:	13
Total “Approximately 81-95% complete”:	8
Total “Approximately 71-80% complete”:	0
Total “Approximately 51-70% complete”:	2
Total " Approximately 0-50% complete ":	2

V. OMB Assessment of Agency Incident Handling Programs

A. Incident Reporting

FISMA requires each agency to document and implement procedures for detecting, reporting and responding to security incidents. Agencies must also notify and consult with the Federal information security incident center operated by the Department of Homeland Security.[6] The Act also requires OMB oversight of the Federal information security incident center and NIST to issue incident detection and handling guidelines.[7]

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

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

In FY 2005, 3569 incidents were reported to the DHS incident response center.

Unauthorized Access	304
Denial of Service	31
Malicious Code	1,806
Improper Usage	370
Scans/Probes/Attempted Access	976
Investigation	82
Total	3,569

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

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

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

Although agencies participated in development of the incident handling concept of operations last year, DHS continues to find sporadic reporting by some agencies and unusually low levels of reporting by others. Less than full reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event, e.g., the widespread propagation of an Internet worm.

In an effort to address this problem, DHS has an automated tool at three agencies and has funding to install it at six others. The tool monitors network flow information and automatically transmits data to DHS. Use of this and similar tools should considerably improve the government's ability to identify incidents and respond in a timely manner. OMB will continue to work with agencies and DHS to ensure appropriate processes and procedures are in place to fully report on security incidents.

B. Incident Detection

In this year's FISMA reporting guidance OMB asked agencies "what tools, techniques, technologies, etc. does the agency use for incident detection?"

The agencies use a variety of technical means to detect incidents and to mitigate Internet risk, including:

- Firewalls;
- Intrusion detection systems;
- E-mail content scanning;
- Access control lists;
- Periodic review of system log records;
- Auditing of system and user activities;
- Antivirus servers;
- Anti-spam software;
- Uniform resource locator (URL) filtering;
- Egress filtering; and
- File integrity checking.

C. Incident prevention

In addition, the agencies routinely implement the following controls in order to prevent incidents.

- Implementation of security configuration standards;
- Vulnerability scans;

- Patch management;
- Penetration tests;
- Use of demilitarized zones;
- Port and protocol oversight;
- Network proxies; and
- Restrictions on active content.

VI. Plan of Action to Improve Performance

A. President's Management Agenda Scorecard

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

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

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of performance in all the criteria), or red (agencies have any one of a number of serious flaws).

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

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

- Inspector General verifies the effectiveness of the Department-wide IT security remediation process;

- Inspector General rates the agency certification and accreditation process as "Satisfactory" or better; and

- The agency has 90% of all IT systems properly secured (certified and accredited).

In order to "maintain green," by July 1, 2006, agencies must have:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations; and
- Consolidated and/or optimized all agency infrastructure to include providing for continuity of operations.

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

B. Review of Agency Business Cases

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

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

Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case justification for major 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 on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

In FY 2005, Federal agencies spent $5.0 billion securing the government's total information technology investment of approximately $62 billion or about eight percent of the total information technology portfolio.

C. Information System Security Line of Business

In FY 2005, the Information System Security Business Task Force identified common solutions to be shared across government and developed a joint business case outlining a general concept of operations with overall milestones and budget estimates. The Task Force identified common solutions in four areas – training, reporting, incident response, and evaluating and selecting security products and services. All agencies were asked to

submit proposals to either become a service provider (Center of Excellence) for other agencies, or migrate to another agency from which they would acquire expert security services. The Department of Homeland Security is continuing to serve as the program manager for this effort and will work with those agencies proposing to become centers of excellence to bring greater clarity to their proposals. OMB intends to achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable.

VII. Conclusion

Over the past year, agencies made steady progress in closing the Federal government's information technology security performance gaps. During this period, the total number of reported systems increased by 19%, from 8623 to 10289.

Analysis of baseline performance measures indicates the following policy compliance improvements:

- 32% increase in the number of systems certified and accredited, from 6607 to 8735;
- 28% increase in the number of systems with tested contingency plans, from 4886 to 6230; and
- Modest increases in the quality of agency certification and accreditation as well as POA&M processes.

However, uneven implementation of security measures across the Federal government leaves weaknesses to be corrected. Through existing processes, OMB will work with agencies to focus management attention on:

- Adherence to NIST publications including NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems;"
- Maintenance of system inventories, security configurations, contingency plans, and contractor oversight; and
- Continued improvement in agencies' certification and accreditation and POA&M processes.

The Administration intends to focus on the implementation of an information security line of business to reduce costs and increase security effectiveness across government. The establishment of Centers of Excellence for security training and FISMA reporting will be a first step towards ensuring greater use of standardized products and services.

OMB will continue to work with agencies, IGs, GAO, and the Congress to strengthen the Federal government's information technology security program.

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

VIII. Additional Information

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

Appendix A: Individual Agency Summaries

In FY 2005, agencies submitted FISMA reports and a corresponding evaluation by the agency Inspector General or a designated independent assessor. This appendix includes a government-wide summary of agency CIO and IG reports, as well as detailed individual agency performance summaries.

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

- Certification and Accreditation;
- Documented Procedures for Using Emerging Technologies;
- Testing of System Security Controls and Contingency Plans;
- Security Awareness, Training and Education;
- Configuration Management and Incident Handling Policies;
- Agency Plan of Action and Milestones Process;
- Security of Contractor Provided Services;
- Quality of the Certification and Accreditation Process; and
- System Inventory Development and Verification.

-This page left blank intentionally.-

Government-wide Summary -- CIO Reports

Total Number of systems	**10289**	
Agency systems	**9184**	
High	1646	
Moderate	2497	
Low	4456	
Not categorized	585	
Contractor systems	**1105**	
High	295	
Moderate	252	
Low	168	
Not categorized	390	
Certified and Accredited Systems - Total	8735	85%
High	1714	88%
Moderate	2357	86%
Low	4111	89%
Not categorized	553	57%
Tested Security Controls - Total	7425	72%
High	1617	83%
Moderate	2086	76%
Low	3318	72%
Not categorized	404	42%
Tested Contingency Plans - Total	6233	61%
High	1200	62%
Moderate	1827	67%
Low	3141	68%
Not categorized	65	7%
Total # of Systems not Categorized	970	9%
Incidents Reported Internally	3,459,172	
Incidents Reported to USCERT	3,447,869	
Incidents Reported to Law Enforcement	6,837	
Total Number of Employees	4,222,251	
Employees that received IT security awareness training	3,427,756	81%
Total Number of Employees with significant IT security responsibilities	107,540	
Employees with significant responsibilities that received training	88,939	83%
Total Costs for providing IT security training	$79,389,201	
The agency explains policies regarding peer-to-peer file sharing in training	Yes: 24 agencies No: 1 agencies	
There is an agency-wide security configuration policy	Yes: 24 agencies No: 1 agency	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes: 21 agencies No: 4 agencies	

-This page left blank intentionally.-

Government-wide Summary -- IG Reports

Quality of agency C&A process	Excellent:	1 agency
	Good:	4 agencies
	Satisfactory:	12 agencies
	Poor:	8 agencies
	Failing:	0 agencies
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance **1 IG - unaudited (DOL)**	Rarely (0-50% of the time):	3 agencies
	Sometimes (51-70% of the time):	3 agencies
	Frequently (71-80% of the time):	3 agencies
	Mostly (81-95% of the time):	5 agencies
	Almost Always (96-100% of the time):	10 agencies
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 0-50% complete:	2 agencies
	Approximately 51-70% complete:	2 agencies
	Approximately 71-80% complete:	0 agencies
	Approximately 81-95% complete:	8 agencies
	Approximately 96-100% complete:	13 agencies
The OIG generally agrees with the CIO on the number of agency owned systems	Yes:	21 agencies
	No:	4 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:	19 agencies
	No:	6 agencies
The agency inventory is maintained and updated at least annually	Yes:	20 agencies
	No:	5 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):	3 agencies
	Sometimes (51-70% of the time):	4 agencies
	Frequently (71-80% of the time):	1 agency
	Mostly (81-95% of the time):	6 agencies
	Almost Always (96-100% of the time):	11 agencies
OIG Findings are incorporated into the POA&M process	Rarely (0-50% of the time):	1 agency
	Sometimes (51-70% of the time):	3 agencies
	Frequently (71-80% of the time):	1 agency
	Mostly (81-95% of the time):	5 agencies
	Almost Always (96-100% of the time):	15 agencies

Effective POA&M process?	Yes:	19 agencies
Note: To arrive at "Effective" as reflected in this Appendix, OMB considers a set of IG responses, including how weaknesses are incorporated in the POA&M, how they are prioritized, and how the status of weaknesses is tracked and reported.	No:	6 agencies
The agency has completed system e-authentication risk assessments	Yes:	15 agencies
1 IG - Unaudited (DOL)	No:	9 agencies
There is an agency wide security configuration policy	Yes:	22 agencies
	No:	3 agencies
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes:	20 agencies
2 IGs - Unaudited (DOC, DoD)	No:	3 agencies
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes:	18 agencies
3 IGs - Unaudited (DOC, DoD, VA)	No:	4 agencies
The agency follows defined procedures for reporting to the USCERT	Yes:	20 agencies
3 IGs - Unaudited (DOC, DoD, VA)	No:	2 agencies

The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Rarely (0-50% of the time):	0 agencies
1 IG - Unaudited (DoD)	Sometimes (51-70% of the time):	5 agencies
	Frequently (71-80% of the time):	0 agencies
	Mostly (81-95% of the time):	11 agencies
	Almost Always (96-100% of the time):	8 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:	22 agencies
	No:	3 agencies

United States Agency for International Development -- CIO Report

Total Number of systems	**9**	
Agency systems	**6**	
High	0	
Moderate	5	
Low	1	
Not categorized	0	
Contractor systems	**3**	
High	0	
Moderate	3	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	9	100%
High	0	0%
Moderate	8	100%
Low	1	100%
Not categorized	0	0%
Tested Security Controls - Total	9	100%
High	0	0%
Moderate	8	100%
Low	1	100%
Not categorized	0	0%
Tested Contingency Plans - Total	9	100%
High	0	0%
Moderate	8	100%
Low	1	100%
Not categorized	0	100%
Total # of Systems not Categorized	0	
Incidents Reported Internally	77	
Incidents Reported to USCERT	77	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	8,339	
Employees that received IT security awareness training	8,339	100%
Total Number of Employees with significant IT security responsibilities	197	
Employees with significant responsibilities that received training	183	93%
Total Costs for providing IT security training	$77,564	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

United States Agency for International Development -- IG Report

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

Department of Agriculture -- CIO Report

Total Number of systems	**462**	
Agency systems	**458**	
High	107	
Moderate	66	
Low	242	
Not categorized	43	
Contractor systems	**4**	
High	0	
Moderate	3	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	420	91%
High	102	95%
Moderate	62	90%
Low	237	98%
Not categorized	19	44%
Tested Security Controls - Total	410	89%
High	95	89%
Moderate	62	90%
Low	235	97%
Not categorized	18	42%
Tested Contingency Plans - Total	314	68%
High	86	80%
Moderate	20	29%
Low	202	83%
Not categorized	6	14%
Total # of Systems not Categorized	43	
Incidents Reported Internally	492	
Incidents Reported to USCERT	58	
Incidents Reported to Law Enforcement	22	
Total Number of Employees	117,128	
Employees that received IT security awareness training	72,890	62%
Total Number of Employees with significant IT security responsibilities	1,125	
Employees with significant responsibilities that received training	658	58%
Total Costs for providing IT security training	$411,827	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of 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	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 0-50% complete
The OIG generally agrees with the CIO on the number of agency owned systems	No
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	No
The agency inventory is maintained and updated at least annually	No
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	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	Sometimes (51-70% 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

Department of Commerce -- CIO Report

Total Number of systems	**345**	
Agency systems	**343**	
High	49	
Moderate	215	
Low	60	
Not categorized	19	
Contractor systems	**2**	
High	0	
Moderate	1	
Low	0	
Not categorized	1	
Certified and Accredited Systems - Total	334	97%
High	49	100%
Moderate	210	97%
Low	58	97%
Not categorized	17	85%
Tested Security Controls - Total	268	78%
High	49	100%
Moderate	152	70%
Low	55	92%
Not categorized	12	60%
Tested Contingency Plans - Total	302	88%
High	46	94%
Moderate	193	89%
Low	60	100%
Not categorized	3	15%
Total # of Systems not Categorized	20	
Incidents Reported Internally	449	
Incidents Reported to USCERT	323	
Incidents Reported to Law Enforcement	1	
Total Number of Employees	43,089	
Employees that received IT security awareness training	42,196	98%
Total Number of Employees with significant IT security responsibilities	1,165	
Employees with significant responsibilities that received training	949	59%
Total Costs for providing IT security training	$1,370,778	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Commerce -- IG Report

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

Department of Defense -- CIO Report

Total Number of systems	**3583**	
Agency systems	**3566**	
High	343	
Moderate	771	
Low	2408	
Not categorized	44	
Contractor systems	**17**	
High	2	
Moderate	8	
Low	7	
Not categorized	0	
Certified and Accredited Systems - Total	2945	82%
High	262	76%
Moderate	593	76%
Low	2053	85%
Not categorized	37	84%
Tested Security Controls - Total	1953	55%
High	185	54%
Moderate	430	55%
Low	1336	55%
Not categorized	2	5%
Tested Contingency Plans - Total	1820	51%
High	158	46%
Moderate	389	50%
Low	1272	53%
Not categorized	1	2%
Total # of Systems not Categorized	44	
Incidents Reported Internally	9,902	
Incidents Reported to USCERT	0	
Incidents Reported to Law Enforcement	734	
Total Number of Employees	2,745,001	
Employees that received IT security awareness training	2,079,957	76%
Total Number of Employees with significant IT security responsibilities	79,986	
Employees with significant responsibilities that received training	67,664	85%
Total Costs for providing IT security training	$42,746,650	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Defense -- IG Report

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

Department of Education -- CIO Report

Total Number of systems	**60**	
Agency systems	**38**	
High	2	
Moderate	0	
Low	36	
Not categorized	0	
Contractor systems	**22**	
High	9	
Moderate	0	
Low	13	
Not categorized	0	
Certified and Accredited Systems - Total	60	100%
High	11	100%
Moderate	0	0%
Low	49	100%
Not categorized	0	0%
Tested Security Controls - Total	60	100%
High	11	100%
Moderate	0	0%
Low	49	100%
Not categorized	0	0%
Tested Contingency Plans - Total	60	100%
High	11	100%
Moderate	0	0%
Low	49	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	171	
Incidents Reported to USCERT	3	
Incidents Reported to Law Enforcement	5	
Total Number of Employees	8072	
Employees that received IT security awareness training	7841	97%
Total Number of Employees with significant IT security responsibilities	526	
Employees with significant responsibilities that received training	441	82%
Total Costs for providing IT security training	$207,157	
The agency explains policies regarding peer-to-peer file sharing in training	No	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of 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	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	No
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of 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

Department of Energy -- CIO Report

Total Number of systems	**787**	
Agency systems	**201**	
High	44	
Moderate	59	
Low	69	
Not categorized	29	
Contractor systems	**586**	
High	159	
Moderate	40	
Low	53	
Not categorized	334	
Certified and Accredited Systems - Total	781	99%
High	202	100%
Moderate	99	100%
Low	117	96%
Not categorized	363	100%
Tested Security Controls - Total	670	85%
High	170	83%
Moderate	68	69%
Low	122	100%
Not categorized	310	85%
Tested Contingency Plans - Total	277	35%
High	64	32%
Moderate	67	68%
Low	118	97%
Not categorized	28	8%
Total # of Systems not Categorized	363	
Incidents Reported Internally	134	
Incidents Reported to USCERT	131	
Incidents Reported to Law Enforcement	131	
Total Number of Employees	139,230	
Employees that received IT security awareness training	131,398	94%
Total Number of Employees with significant IT security responsibilities	2,406.50	
Employees with significant responsibilities that received training	2,354.00	98%
Total Costs for providing IT security training	$10,472,435	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Department of Energy -- IG Report

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

Environmental Protection Agency -- CIO Report

Total Number of systems	**167**	
Agency systems	**155**	
High	16	
Moderate	100	
Low	39	
Not categorized	0	
Contractor systems	**12**	
High	0	
Moderate	6	
Low	6	
Not categorized	0	
Certified and Accredited Systems - Total	167	100%
High	16	100%
Moderate	106	100%
Low	45	100%
Not categorized	0	0%
Tested Security Controls - Total	161	96%
High	16	100%
Moderate	104	98%
Low	41	91%
Not categorized	0	0%
Tested Contingency Plans - Total	162	97%
High	16	100%
Moderate	104	98%
Low	42	93%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	833	
Incidents Reported to USCERT	833	
Incidents Reported to Law Enforcement	2	
Total Number of Employees	22,479	
Employees that received IT security awareness training	21,454	95%
Total Number of Employees with significant IT security responsibilities	620	
Employees with significant responsibilities that received training	468	75%
Total Costs for providing IT security training	$527,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Environmental Protection Agency -- IG Report

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

General Services Administration -- CIO Report

Total Number of systems	**84**	
Agency systems	**48**	
High	0	
Moderate	33	
Low	15	
Not categorized	0	
Contractor systems	**36**	
High	0	
Moderate	20	
Low	16	
Not categorized	0	
Certified and Accredited Systems - Total	84	100%
High	0	0%
Moderate	53	100%
Low	31	100%
Not categorized	0	0%
Tested Security Controls - Total	83	99%
High	0	0%
Moderate	53	100%
Low	30	97%
Not categorized	0	0%
Tested Contingency Plans - Total	55	66%
High	0	0%
Moderate	36	68%
Low	19	61%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	12	
Incidents Reported to USCERT	11	
Incidents Reported to Law Enforcement	1	
Total Number of Employees	17,369	
Employees that received IT security awareness training	17,369	100%
Total Number of Employees with significant IT security responsibilities	1,065	
Employees with significant responsibilities that received training	1,024	96%
Total Costs for providing IT security training	$270,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

General Services Administration -- IG Report

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

Department of Health and Human Services -- CIO Report

Total Number of systems	**177**	
Agency systems	**165**	
High	48	
Moderate	68	
Low	49	
Not categorized	0	
Contractor systems	**12**	
High	2	
Moderate	5	
Low	5	
Not categorized	0	
Certified and Accredited Systems - Total	175	99%
High	49	98%
Moderate	73	100%
Low	53	98%
Not categorized	0	0%
Tested Security Controls - Total	161	91%
High	49	98%
Moderate	71	97%
Low	41	76%
Not categorized	0	0%
Tested Contingency Plans - Total	143	81%
High	50	100%
Moderate	58	80%
Low	35	65%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	165	
Incidents Reported to USCERT	64	
Incidents Reported to Law Enforcement	24	
Total Number of Employees	73,383	
Employees that received IT security awareness training	72,250	98%
Total Number of Employees with significant IT security responsibilities	1,308	
Employees with significant responsibilities that received training	885	68%
Total Costs for providing IT security training	$1,145,826	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Health and Human Services -- IG Report

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

Department of Homeland Security -- CIO Report

Total Number of systems	**764**	
Agency systems	**543**	
High	280	
Moderate	88	
Low	19	
Not categorized	156	
Contractor systems	**221**	
High	73	
Moderate	77	
Low	23	
Not categorized	48	
Certified and Accredited Systems - Total	327	43%
High	247	70%
Moderate	66	40%
Low	13	31%
Not categorized	1	1%
Tested Security Controls - Total	397	52%
High	281	80%
Moderate	87	53%
Low	19	45%
Not categorized	10	5%
Tested Contingency Plans - Total	65	9%
High	41	12%
Moderate	21	13%
Low	3	7%
Not categorized	0	0%
Total # of Systems not Categorized	204	
Incidents Reported Internally	423	
Incidents Reported to USCERT	423	
Incidents Reported to Law Enforcement	57	
Total Number of Employees	188,167	
Employees that received IT security awareness training	165,847	88%
Total Number of Employees with significant IT security responsibilities	1,142	
Employees with significant responsibilities that received training	1,109	97%
Total Costs for providing IT security training	$3,065,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Homeland Security -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	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	Sometimes (51-70% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	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	No

Department of Housing and Urban Development -- CIO Report

Total Number of systems	**154**	
Agency systems	**143**	
High	54	
Moderate	46	
Low	43	
Not categorized	0	
Contractor systems	**11**	
High	4	
Moderate	7	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	141	92%
High	54	93%
Moderate	45	85%
Low	42	98%
Not categorized	0	0%
Tested Security Controls - Total	141	92%
High	54	93%
Moderate	45	85%
Low	42	98%
Not categorized	0	0%
Tested Contingency Plans - Total	40	26%
High	25	43%
Moderate	11	21%
Low	4	9%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	0	
Incidents Reported to USCERT	1	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	9,602	
Employees that received IT security awareness training	9,104	95%
Total Number of Employees with significant IT security responsibilities	273	
Employees with significant responsibilities that received training	270	99%
Total Costs for providing IT security training	$55,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Housing and Urban Development -- IG Report

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

Department of the Interior -- CIO Report

Total Number of systems	**166**	
Agency systems	**156**	
High	21	
Moderate	117	
Low	18	
Not categorized	0	
Contractor systems	**10**	
High	4	
Moderate	5	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	163	98%
High	24	96%
Moderate	121	99%
Low	18	95%
Not categorized	0	0%
Tested Security Controls - Total	161	97%
High	24	96%
Moderate	119	98%
Low	18	95%
Not categorized	0	0%
Tested Contingency Plans - Total	156	94%
High	24	96%
Moderate	115	94%
Low	17	90%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	286	
Incidents Reported to USCERT	251	
Incidents Reported to Law Enforcement	10	
Total Number of Employees	84,159	
Employees that received IT security awareness training	82,848	98%
Total Number of Employees with significant IT security responsibilities	2,611	
Employees with significant responsibilities that received training	1,736	66%
Total Costs for providing IT security training	$1,340,487	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of the Interior -- IG Report

Quality of agency C&A process	Poor
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Frequently (71-80% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	Mostly (81-95% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	No
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	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

Department of Justice -- CIO Report

Total Number of systems	**215**	
Agency systems	**210**	
High	129	
Moderate	53	
Low	28	
Not categorized	0	
Contractor systems	**5**	
High	5	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	213	99%
High	134	100%
Moderate	53	100%
Low	26	93%
Not categorized	0	0%
Tested Security Controls - Total	208	97%
High	129	96%
Moderate	52	98%
Low	27	96%
Not categorized	0	0%
Tested Contingency Plans - Total	214	100%
High	133	99%
Moderate	53	100%
Low	28	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	2,396	
Incidents Reported to USCERT	2,395	
Incidents Reported to Law Enforcement	5	
Total Number of Employees	116,501	
Employees that received IT security awareness training	112,216	96%
Total Number of Employees with significant IT security responsibilities	3,469	
Employees with significant responsibilities that received training	3,391	98%
Total Costs for providing IT security training	$5,394,300	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	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

Department of Labor -- CIO Report

Total Number of systems	**85**	
Agency systems	**76**	
High	0	
Moderate	65	
Low	11	
Not categorized	0	
Contractor systems	**9**	
High	0	
Moderate	6	
Low	3	
Not categorized	0	
Certified and Accredited Systems - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Tested Security Controls - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Tested Contingency Plans - Total	85	100%
High	0	0%
Moderate	71	100%
Low	14	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	32	
Incidents Reported to USCERT	0	
Incidents Reported to Law Enforcement	4	
Total Number of Employees	17,160	
Employees that received IT security awareness training	16,058	94%
Total Number of Employees with significant IT security responsibilities	853	
Employees with significant responsibilities that received training	799	94%
Total Costs for providing IT security training	$271,445	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of Labor -- IG Report

Quality of agency C&A process	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	Unaudited
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Unaudited
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 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

National Aeronautics and Space Administration -- CIO Report

Total Number of systems	**1354**	
Agency systems	**1266**	
High	59	
Moderate	260	
Low	936	
Not categorized	11	
Contractor systems	**88**	
High	16	
Moderate	42	
Low	30	
Not categorized	0	
Certified and Accredited Systems - Total	1255	93%
High	59	79%
Moderate	260	86%
Low	936	97%
Not categorized	0	0%
Tested Security Controls - Total	1227	91%
High	59	79%
Moderate	260	86%
Low	908	94%
Not categorized	0	0%
Tested Contingency Plans - Total	1230	91%
High	59	79%
Moderate	260	86%
Low	911	94%
Not categorized	0	0%
Total # of Systems not Categorized	11	
Incidents Reported Internally	108	
Incidents Reported to USCERT	108	
Incidents Reported to Law Enforcement	32	
Total Number of Employees	57,278	
Employees that received IT security awareness training	56,968	99%
Total Number of Employees with significant IT security responsibilities	2,761	
Employees with significant responsibilities that received training	2,753	99%
Total Costs for providing IT security training	$1,300,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Aeronautics and Space Administration -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Sometimes (51-70% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of 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

National Science Foundation -- CIO Report

Total Number of systems	**19**	
Agency systems	**16**	
High	4	
Moderate	8	
Low	4	
Not categorized	0	
Contractor systems	**3**	
High	2	
Moderate	1	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Security Controls - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Tested Contingency Plans - Total	19	100%
High	6	100%
Moderate	9	100%
Low	4	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	4	
Incidents Reported to USCERT	4	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	4,413	
Employees that received IT security awareness training	4,242	96%
Total Number of Employees with significant IT security responsibilities	22	
Employees with significant responsibilities that received training	9	41%
Total Costs for providing IT security training	$74,765	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

National Science Foundation -- IG Report

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

Nuclear Regulatory Commission -- CIO Report

Total Number of systems	**34**	
Agency systems	**27**	
High	4	
Moderate	4	
Low	0	
Not categorized	19	
Contractor systems	**7**	
High	0	
Moderate	0	
Low	0	
Not categorized	7	
Certified and Accredited Systems - Total	11	32%
High	1	25%
Moderate	0	0%
Low	0	0%
Not categorized	10	39%
Tested Security Controls - Total	33	97%
High	4	100%
Moderate	4	100%
Low	0	0%
Not categorized	25	96%
Tested Contingency Plans - Total	6	18%
High	0	0%
Moderate	1	25%
Low	0	0%
Not categorized	5	19%
Total # of Systems not Categorized	26	
Incidents Reported Internally	20,018	
Incidents Reported to USCERT	20,018	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	3,235	
Employees that received IT security awareness training	3,188	99%
Total Number of Employees with significant IT security responsibilities	153	
Employees with significant responsibilities that received training	47	31%
Total Costs for providing IT security training	$107,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Nuclear Regulatory Commission -- IG Report

Quality of agency C&A process	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 51-70% complete
The OIG generally agrees with the CIO on the number of agency owned systems	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	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	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Mostly (81-95% of 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

Office of Personnel Management -- CIO Report

Total Number of systems	**57**	
Agency systems	**57**	
High	12	
Moderate	13	
Low	24	
Not categorized	8	
Contractor systems	**0**	
High	0	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	57	100%
High	12	100%
Moderate	13	100%
Low	24	100%
Not categorized	8	100%
Tested Security Controls - Total	57	100%
High	12	100%
Moderate	13	100%
Low	24	100%
Not categorized	8	100%
Tested Contingency Plans - Total	57	100%
High	12	100%
Moderate	13	100%
Low	24	100%
Not categorized	8	100%
Total # of Systems not Categorized	8	
Incidents Reported Internally	0	
Incidents Reported to USCERT	0	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	4,513	
Employees that received IT security awareness training	4,513	100%
Total Number of Employees with significant IT security responsibilities	57	
Employees with significant responsibilities that received training	55	96%
Total Costs for providing IT security training	$53,402	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency 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 indentification of interfaces (including those not under control of the agency)	Approximately 96-100% complete
The OIG generally agrees with the CIO on the number of agency owned systems	Yes
The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency	Yes
The agency inventory is maintained and updated at least annually	Yes
The POA&M is an agency wide process, incorporating all known IT Security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	Almost Always (96-100% of the time)
OIG Findings are incorporated into the POA&M process	Almost Always (96-100% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Almost Always (96-100% of 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

Small Business Administration -- CIO Report

Total Number of systems	**20**	
Agency systems	**13**	
High	1	
Moderate	12	
Low	0	
Not categorized	0	
Contractor systems	**7**	
High	4	
Moderate	3	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	20	100%
High	5	100%
Moderate	15	100%
Low	0	0%
Not categorized	0	0%
Tested Security Controls - Total	20	100
High	5	100%
Moderate	15	100%
Low	0	0%
Not categorized	0	0%
Tested Contingency Plans - Total	18	90%
High	5	100%
Moderate	13	87%
Low	0	0%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	3,422,779	
Incidents Reported to USCERT	3,422,779	
Incidents Reported to Law Enforcement	5,837	
Total Number of Employees	4,663	
Employees that received IT security awareness training	3,104	67%
Total Number of Employees with significant IT security responsibilities	122	
Employees with significant responsibilities that received training	84	69%
Total Costs for providing IT security training	$52,064	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

Small Business Administration -- IG Report

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

Smithsonian Institution -- CIO Report

Total Number of systems	**14**	
Agency systems	**14**	
High	0	
Moderate	4	
Low	10	
Not categorized	0	
Contractor systems	**0**	
High	0	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	14	100%
High	0	0%
Moderate	4	100%
Low	10	100%
Not categorized	0	0%
Tested Security Controls - Total	14	100%
High	0	0%
Moderate	4	100%
Low	10	100%
Not categorized	0	0%
Tested Contingency Plans - Total	14	100%
High	0	0%
Moderate	4	100%
Low	10	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	2	
Incidents Reported to USCERT	2	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	7,530	
Employees that received IT security awareness training	6,577	87%
Total Number of Employees with significant IT security responsibilities	81	
Employees with significant responsibilities that received training	49	46%
Total Costs for providing IT security training	$22,300	
The agency explains policies regarding peer-to-peer file sharing in training	yes	
There is an agency-wide security configuration policy	yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	yes	

Smithsonian Institution -- IG Report

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

Social Security Administration -- CIO Report

Total Number of systems	**20**	
Agency systems	**20**	
High	0	
Moderate	7	
Low	13	
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	7	100%
Low	13	100%
Not categorized	0	0%
Tested Security Controls - Total	20	100%
High	0	0%
Moderate	7	100%
Low	13	100%
Not categorized	0	0%
Tested Contingency Plans - Total	20	100%
High	0	0%
Moderate	7	100%
Low	13	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	0	
Incidents Reported to USCERT	0	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	67,331	
Employees that received IT security awareness training	67,331	100%
Total Number of Employees with significant IT security responsibilities	875	
Employees with significant responsibilities that received training	816	93%
Total Costs for providing IT security training	$943,989	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Social Security Administration -- IG Report

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

Department of State -- CIO Report

Total Number of systems	**431**	
Agency systems	**431**	
High	21	
Moderate	58	
Low	112	
Not categorized	240	
Contractor systems	**0**	
High	0	
Moderate	0	
Low	0	
Not categorized	0	
Certified and Accredited Systems - Total	188	44%
High	15	71%
Moderate	44	76%
Low	38	34%
Not categorized	91	38%
Tested Security Controls - Total	31	7%
High	6	29%
Moderate	9	16%
Low	5	5%
Not categorized	11	5%
Tested Contingency Plans - Total	18	4%
High	6	29%
Moderate	3	5%
Low	3	3%
Not categorized	6	3%
Total # of Systems not Categorized	240	
Incidents Reported Internally	4	
Incidents Reported to USCERT	2	
Incidents Reported to Law Enforcement	4	
Total Number of Employees	70,644	
Employees that received IT security awareness training	48,968	69%
Total Number of Employees with significant IT security responsibilities	2,132	
Employees with significant responsibilities that received training	1,106	52%
Total Costs for providing IT security training	$2,433,919	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of State -- IG Report

Quality of agency C&A process	Satisfactory
The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB Policy and NIST guidance	Rarely (0-50% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	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	Sometimes (51-70% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Sometimes (51-70% 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

Department of Transportation -- CIO Report

Total Number of systems	**451**	
Agency systems	**411**	
High	95	
Moderate	227	
Low	80	
Not categorized	9	
Contractor systems	**40**	
High	11	
Moderate	21	
Low	8	
Not categorized	0	
Certified and Accredited Systems - Total	432	96%
High	106	100%
Moderate	232	94%
Low	88	100%
Not categorized	6	67%
Tested Security Controls - Total	428	95%
High	106	100%
Moderate	229	92%
Low	87	99%
Not categorized	6	67%
Tested Contingency Plans - Total	400	89%
High	106	100%
Moderate	213	86%
Low	75	85%
Not categorized	6	67%
Total # of Systems not Categorized	9	
Incidents Reported Internally	845	
Incidents Reported to USCERT	353	
Incidents Reported to Law Enforcement	17	
Total Number of Employees	56,414	
Employees that received IT security awareness training	53,931	96%
Total Number of Employees with significant IT security responsibilities	560	
Employees with significant responsibilities that received training	556	99%
Total Costs for providing IT security training	$571,372	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	No	

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

Department of the Treasury -- CIO Report

Total Number of systems	**241**	
Agency systems	**234**	
High	35	
Moderate	180	
Low	17	
Not categorized	2	
Contractor systems	**7**	
High	4	
Moderate	2	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	230	95%
High	38	97%
Moderate	173	95%
Low	18	100%
Not categorized	1	50%
Tested Security Controls - Total	224	93%
High	34	87%
Moderate	174	96%
Low	14	78%
Not categorized	2	100%
Tested Contingency Plans - Total	164	68%
High	30	77%
Moderate	118	65%
Low	14	78%
Not categorized	2	100%
Total # of Systems not Categorized	2	
Incidents Reported Internally	33	
Incidents Reported to USCERT	26	
Incidents Reported to Law Enforcement	0	
Total Number of Employees	124,984	
Employees that received IT security awareness training	123,007	99%
Total Number of Employees with significant IT security responsibilities	3,258	
Employees with significant responsibilities that received training	760	23%
Total Costs for providing IT security training	$3,481,921	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	Yes	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	Yes	

Department of the Treasury -- IG Report

Quality of agency C&A process	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	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	Rarely (0-50% of the time)
OIG Findings are incorporated into the POA&M process	Sometimes (51-70% of the time)
Effective POA&M process?	No
The agency has completed system e-authentication risk assessments	Yes
There is an agency wide security configuration policy	Yes
The agency follows documented policies and procedures for identifying and reporting incidents internally	Yes
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Yes
The agency follows defined procedures for reporting to the USCERT	Yes
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	Sometimes (51-70% 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

Department of Veterans Affairs -- CIO Report

Total Number of systems	**585**	
Agency systems	**582**	
High	322	
Moderate	38	
Low	222	
Not categorized	0	
Contractor systems	**3**	
High	0	
Moderate	2	
Low	1	
Not categorized	0	
Certified and Accredited Systems - Total	585	100%
High	322	100%
Moderate	40	100%
Low	223	100%
Not categorized	0	0%
Tested Security Controls - Total	585	100%
High	322	100%
Moderate	40	100%
Low	223	100%
Not categorized	0	0%
Tested Contingency Plans - Total	585	100%
High	322	100%
Moderate	40	100%
Low	223	100%
Not categorized	0	0%
Total # of Systems not Categorized	0	
Incidents Reported Internally	7	
Incidents Reported to USCERT	7	
Incidents Reported to Law Enforcement	1	
Total Number of Employees	231,567	
Employees that received IT security awareness training	216,160	93%
Total Number of Employees with significant IT security responsibilities	773	
Employees with significant responsibilities that received training	773	100%
Total Costs for providing IT security training	$2,993,000	
The agency explains policies regarding peer-to-peer file sharing in training	Yes	
There is an agency-wide security configuration policy	No	
The agency has documented in its security policies special procedures for using emerging technologies and countering emerging threats	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	Mostly (81-95% of the time)
The agency has developed an inventory of major information systems, including an indentification of interfaces (including those not under control of the agency)	Approximately 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	Mostly (81-95% of the time)
OIG Findings are incorporated into the POA&M process	Mostly (81-95% of the time)
Effective POA&M process?	Yes
The agency has completed system e-authentication risk assessments	No
There is an agency wide security configuration policy	No
The agency follows documented policies and procedures for identifying and reporting incidents internally	No
The agency follows documented policies and procedures for external reporting to law enforcement authorities	Unaudited
The agency follows defined procedures for reporting to the USCERT	Unaudited
The agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities	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

Appendix B: Reporting by Small and Independent Agencies

Background

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

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

Chief Information Officers (CIO) from the small and independent agencies participate in the Small Agency CIO Council which in turn is represented on the Federal CIO Council chaired by OMB. During FY 2005, the Small Agency CIO Council worked with OMB to assist small agencies in complying with FISMA. On June 17, 2005, the Council invited all small agency CIOs and IGs to attend a special FISMA workshop. OMB staff briefed the group on FISMA requirements and the latest security guidelines. The Council also invited a noted private sector independent auditor to this workshop to lead a discussion on how micro-agencies can improve their audits. We also had several agencies lead discussions on software tools that can assist agency staff in managing FISMA compliance. The workshop was very helpful because it allowed individual agency IGs and CIOs to exchange ideas and best practices on how to conduct the FISMA review within the context of a small agency program.

FISMA Reporting Requirements and Results

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

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

In FY 2005, 53 small and independent agencies submitted FISMA reports. Of the 343 moderate-to-high impact systems reported:

- 90% of systems have security controls that were reviewed in the last year;
- 86% of systems have security controls that were tested and evaluated in the last year;
- 62% of systems have been certified and accredited; and
- 56% of systems have tested contingency plans.

These statistics show that in some areas, small agencies lag behind the larger agencies in key performance metric areas. Through efforts such as the Information System Security Line of Business, we intend to make progress in closing these gaps.

Independent Assessments. 48 small and independent agencies conducted independent assessments of their systems in FY 2005 (91% compared to 72% last year).

Implementation of NIST SP 800-53. 81% of small and independent agencies reported that they have begun to implement security controls in NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems".

Certification and Accreditation. 21 small and independent agencies (40%) have certified and accredited all of their systems. This represents a 24% increase over FY 2004, when 30 percent of agencies reported success.

Testing of Agency and Contractor Security Controls. 31 small and independent agencies (59%) reported that all agency and contractor systems' security controls were tested by FIPS-199 categorization in FY 2005. Only 44% of agencies tested all of their controls in FY 2004.

Systems Categorized by FIPS-199. 38 small and independent agencies (72%) reported that all of their systems have been categorized by FIPS-199.

Incident Reporting to US-CERT. Although almost all small and independent agencies have policies requiring incident reporting to DHS, some fail to characterize abnormal system activity as reportable incidents. Only 14 small and independent agencies (27%) reported at least one abnormal system activity to the US-CERT in FY 2005.

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

> *For All Agency Employees Including Contractors.* 16 small and independent agencies (30%) provided computer security awareness and training to 100% of their employees and contractors. 34 small and independent agencies (64%) provided computer security awareness and training to at least 90% of their employees and contractors. 40 small and independent agencies (76%) provided computer security awareness and training to at least 80% of their employees and contractors.
>
> *For Employees with Significant Security Responsibilities.* 19 small and independent agencies (36%) provided specialized computer security awareness and training to at least 100% of their employees and contractors with significant security responsibilities. 23 small and independent agencies (43%) provided specialized computer security awareness and training to at least 80% of their employees and contractors with significant security responsibilities.

Tested Contingency Plans. 38 small and independent agencies (28%) reported that all of their systems have tested contingency plans. This represents a modest increase over last year's performance, when only 25% of agencies reported success.

Contractor Systems Reviewed. Of the 31 small and independent agencies with contractor systems, 20 (65%) had all contractor systems reviewed in FY 2005.

Small and Independent Agencies Submitting FISMA Reports in FY 2005

1. African Development Foundation
2. American Battle Monuments Commission
3. Appalachian Regional Commission
4. Barry Goldwater Scholarship Foundation
5. Broadcasting Board of Governors
6. Committee for Purchase From People Who Are Blind or Severely Disabled
7. Corporation for National & Community Service
8. Court Services & Offender Supervision Agency
9. Defense Nuclear Facilities Safety Board
10. Executive Office of the President
11. Export-Import Bank
12. Farm Credit Administration
13. Federal Communications Commission
14. Federal Deposit Insurance Corporation
15. Federal Energy Regulatory Commission
16. Federal Housing Finance Board
17. Federal Maritime Commission
18. Federal Reserve System
19. Federal Retirement Thrift Investment Board
20. Federal Trade Commission
21. Institute of Museum and Library Services
22. Inter-American Foundation
23. Japan-US Friendship Commission
24. Millennium Challenge Corporation
25. Morris K. Udall Foundation
26. National Archives and Records Administration
27. National Credit Union Administration
28. National Endowment for the Arts
29. National Endowment for the Humanities
30. National Gallery of Art
31. National Labor Relations Board
32. National Transportation Safety Board
33. Nuclear Waste Technical Review Board
34. Office of Federal Housing Enterprise Oversight
35. Overseas Private Investment Corporation
36. Peace Corps
37. Pension Benefit Guaranty Corporation

38. Securities and Exchange Commission
39. Selective Service System
40. Tennessee Valley Authority
41. US Chemical Safety and Hazard Investigation Board
42. US Commodity Futures Trading Commission
43. US Consumer Product Safety Commission
44. US Equal Employment Opportunity Commission
45. US Holocaust Memorial Museum
46. US International Trade Commission
47. US Merit Systems Protection Board
48. US Nuclear Waste Technical Review Board
49. US Occupational Safety and Health Review Commission
50. US Office of Government Ethics
51. US Office of Special Counsel
52. US Railroad Retirement Board
53. US Trade and Development Agency

Appendix C: Federal Government's Information Technology Security Program

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

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

Federal National Security Systems

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

Federal Non-National Security Systems

The Office of Management and Budget (OMB) is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security. The National Institute of Standards and Technology (NIST) works collaboratively with OMB to develop standards and guidelines for Federal computer systems in order to achieve cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate. Moreover, both NIST and OMB are encouraged, and in some cases required, to coordinate with NSA "to assure, to the maximum extent feasible, that such standards and guidelines [for non-

National Security Systems] are complementary with standards and guidelines developed for National Security Systems."

Non-Federal Systems

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

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

Statutory Requirements for Federal Non-National Security Systems

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

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

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

- The Federal Information Security Management Act of 2002. FISMA reauthorized the provisions found in the Government Information Security Reform Act and amended the Paperwork Reduction Act of 1995. FISMA generally codifies OMB's security policies and continues the framework established in prior statute, while requiring annual agency program and system reviews, independent IG evaluations, annual agency reports to OMB, and an annual OMB report to Congress. It also requires OMB to annually approve or disapprove agency programs. Additionally, FISMA emphasizes accountability for agency officials' security responsibilities. For example, the role of agency program officials in ensuring the systems supporting their operations and assets are appropriately secure is clearly defined.

Federal Agencies with Specific Information Technology Security Responsibilities

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

1. Policy and Guidance Authorities

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

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

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

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

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

- Promote, measure, and validate security in systems and services;

- Educate consumers; and
- Establish minimum security requirements for Federal systems.

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

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

The Computer Security Division's 2004 Annual Report can be found at: http://csrc.nist.gov/publications/nistir/NISTIR7219-CSD-2004-Annual-Report.pdf. The 2004 annual report highlights the publication of standards and guidelines which provide the foundation for strong information security programs for unclassified Federal information and information systems. In addition, the report discusses NIST's outreach program to promote the understanding of IT security vulnerabilities and corrective measures.

In FY 2005, the Computer Security Division was actively engaged in the following activities:

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

Cryptographic Standards and Applications
Focus is on developing cryptographic methods for protecting the integrity, confidentiality, and authenticity of information resources; and addresses such technical areas as: secret and public key cryptographic techniques; advanced authentication systems; cryptographic protocols and interfaces; public key certificate management; smart tokens; cryptographic key escrowing; and security architectures. Helps enable implementation of cryptographic services in applications and the national infrastructure. Current projects include:

- Advanced Encryption Standard (AES);
- Cryptographic Standards Toolkit;
- Encryption Key Recovery and S/MIME;
- Personal Identity Verification (PIV) of Federal Employees and Contractors; and
- Public Key Infrastructure (PKI).

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

- Automated Security Functional Testing;
- Common Criteria for IT Security Evaluation;
- Cryptographic Module Validation Program (CMVP);
- Internet Protocol Security (IPSec);
- National Information Assurance Partnership (NIAP); and
- National Vulnerability Database (NVD).

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

- Automated Security Functional Testing;
- Authorization Management and Advanced Access Control Models;
- Critical Infrastructure Grants Program;
- Internet Protocol Security (IPSec);
- Mobile Ad Hoc Network Security (MANET);
- Mobile Security;
- Personal Identity Verification (PIV) of Federal Employees and Contractors;
- Smart Card Security and Research;
- SPAM Technology Workshop; and
- Wireless Security.

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

- Automated Security Self-Assessment Tool (ASSET);

- Awareness, Training and Education (ATE);
- Computer Security Guidance (publications);
- Federal Information Processing Standards Publications (FIPS Pubs);
- Computer Security Resource Center (CSRC);
- Federal Agency Security Practices (FASP);
- Federal Computer Security Program Managers' Forum;
- Federal Information Security Management Act (FISMA) Implementation Project;
- Federal Information Systems Security Educators' Association (FISSEA);
- Information Security and Privacy Advisory Board (ISPAB);
- Personal Identity Verification (PIV) of Federal Employees and Contractors;
- Policies (Federal Requirements);
- Practices and Checklists Implementation Guides; and
- Program Review for Information Security Management Assistance (PRISMA).

Selected NIST Special Publications (Issued in FY 2005)

- SP 800-86 (Draft), "Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response"

- SP 800-84 (Draft), "Guide to Single-Organization IT Exercises"

- SP 800-81 (Draft), "Secure Domain Name System (DNS) Deployment Guide"

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

- SP 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," April 2005

- SP 800-77 (Draft), "Guide to IPsec VPNs"

- SP 800-76 (Draft), "Biometric Data Specification for Personal Identity Verification"

- SP 800-73, "Interfaces for Personal Identity Verification," April 2005

- SP 800-72, "Guidelines on PDA Forensics," November 2004

- SP 800-70, "The NIST Security Configuration Checklists Program," May 2005

- SP 800-67, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," May 2004

- SP 800-65, "Integrating Security into the Capital Planning and Investment Control Process," January 2005

2. Assistance, Advice and Operations

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

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

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

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

- Inform operators of agency information systems about current and potential information security threats and vulnerabilities. In FY 2005, US-CERT issued twenty-one Technical Cyber Security Alerts providing timely information about current security issues, vulnerabilities, and exploits. Agency officials were provided a description of the vulnerability, its impact, and the actions required to prevent exploitation of the weakness. Cyber Security Bulletins provide weekly summaries of security issues and new vulnerabilities. They also provide patches, workarounds, and other actions to help mitigate risk. Additionally, US-CERT published eleven non-technical Cyber Security Alerts which provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate computer users can take to protect themselves from attack.

- Compile and analyze information about incidents that threaten information security. US-CERT maintains a close working relationship with the major software manufacturers, Carnegie Mellon's Computer Emergency Response Team (CERT) and the law enforcement and intelligence communities. These parties work together to analyze malicious code and attribute attacks. In FY 2005, agencies reported 3,569 incidents. US-CERT shared information regarding these incidents with Federal agencies, including members of the

Government Forum of Incident Response and Security Teams (GFIRST). DHS created GFIRST in January 2004 as a community of Federal agency emergency computer response teams.

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

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