Federal Information Security Management Act (FISMA)

2004 Report to Congress

Office of Management and Budget
March 1, 2005

TABLE OF CONTENTS

Executive Summary

The Federal Information Security Management Act of 2002

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the Electronic Government Act of 2002. 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 2004, the Federal agencies spent $4.2 billion securing the government's total information technology investment of approximately $59 billion or about seven percent of the total information technology portfolio.

The Act 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. The report is based primarily on agency and IG reports submitted to OMB in October 2004.

This report to Congress provides:

- A summary of government-wide performance in the area of information technology security management
- An analysis of government-wide weaknesses in information technology security practices, and,
- A plan of action to improve information technology security performance

Progress in Meeting Key Security Performance Measures

The report to Congress examines agency status against key security performance measures from FY 2002 through FY 2004. These measures were originally selected because they represent most of the significant information technology security issues for Federal agencies. Agencies have demonstrated significant progress in each:

- Certification and accreditation of systems. In FY 2004, 77% of Federal systems underwent risk assessment and testing of security controls, resulting in an official management approval to operate. In FY 2003, this was 62%. Several agencies have made outstanding progress in FY 2004. The Department of Labor moved from 58% to 96% of systems certified and accredited and the Department of Transportation improved from 33% to 98%.

- "Built-in" security costs. In FY 2004, 85% of systems had security costs incorporated into the system lifecycle planning costs. In FY 2003, this was 77%.

- Annual testing of system controls. In FY 2004, 76% percent of all systems had their management, operational and technical controls tested. This was 64% in 2003.

- Contingency planning. In FY 2004, 75% of systems had contingency plans designed to ensure continuity of operations. Of these, 57% were tested. In 2003, 68% of systems had contingency plans, and only 48% were tested.

- Implementation of security configuration requirements. In FY 2004, for the first time, agencies reported on the degree to which they implemented security configurations for operating systems and software applications. All agencies have begun developing and implementing security configuration policies for at least some of their operating systems.

Below is a summary table showing progress from the baseline comparing FY 2002, FY 2003, and FY 2004 for the number and percentage of agency systems having:

- Authorization to process following certification and accreditation
- Security control costs “built into” the life cycle of the system
- Security controls tested and evaluated in the past year, and,
- Contingency plans tested in the past year

Overall Security Status and Progress from FY2002 to FY2004

	FY02	FY03	**FY04**
Number of Systems and Percentage of Systems* with:			
Effective Security and Privacy Controls (C&A)	3772 47%	4969 62%	**6607** **77%**
“Built in” Security Costs	4919 62%	6182 77%	**7295** **85%**
Tested Security Controls	4751 60%	5143 64%	**6515** **76%**
Tested Contingency Plans	2768 35%	3835 48%	**4886** **57%**

*Total number of systems reported: FY2002= 7957; FY03= 7998; FY2004= 8623. The system count changes as agencies refine their system inventory and acquire, consolidate, or retire systems.

Continuing Security Challenges

While progress has been made, agency IGs continue to identify deficiencies in security policy, procedure and practice. Continuing weaknesses reflect the complexity of securing the Federal government's vast number of information systems. Examples of common deficiencies noted by IGs include:

- Agency-wide Plans of Action and Milestones (POA&Ms). OMB asked agency IGs to assess, against specific criteria, the quality of the agency-wide POA&M process. OMB policy requires agencies to prepare POA&Ms for all programs and systems where a security weakness has been found. Although 18 IGs have verified their agency's management of an effective POA&M process, six IGs revealed overall deficiencies in their agency's process.

- Quality of certification and accreditation process. This year for the first time, IGs were asked to assess the overall quality of their agency's certification and accreditation process, including the degree to which agencies follow NIST guidance. Six IGs rated the agency certification and accreditation process as "good", and nine rated it as "satisfactory"; however, seven IGs rated the process as "poor" and two were not able to complete the evaluation. None of the IGs rated the certification and accreditation process as failing.

Conclusion

The Federal government continues to make significant progress in identifying and addressing its security weaknesses. However, much work remains and OMB will continue to work with agencies, IGs, GAO, and the Congress to strengthen the Federal government's information technology security program and improve compliance with FISMA.

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

I. Introduction

A. Security Legislation

The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for securing the Federal government's information technology. The Act directs the National Institute of Standards and Technology (NIST) to develop information technology security standards and guidelines and each agency to implement an information security program. In addition, the Act requires that the Office of Management and Budget (OMB) oversee information technology security policies and practices across the Federal enterprise.

Agencies must report annually to OMB on the effectiveness of their information technology security programs. The reports must include an independent evaluation by either the agency Inspector General or an external auditor.

B. Purpose and Scope of OMB's Annual FISMA Report

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 2004.

This report is based primarily on FY 2004 agency and IG reports to OMB. Appendix A contains statistical summaries of security performance within the twenty-four Chief Financial Officer Act 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 Guidance

A. FY 2004 FISMA Reporting Instructions

In August 2004, OMB issued M-04-25 “FY2004 Reporting Instructions for the Federal Information Security Management Act” to promote consistent reporting across the government. As in the past, it included quantitative performance measures for the major provisions of FISMA, helping to determine agency status and progress. Many of this year’s performance measures are identical to past years’ guidance and thus changes from the prior baseline are easily discernable.

FISMA requires agencies to report annually to OMB on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of the Act. OMB’s reporting guidance directs agencies to provide an overall view of their security program as well as an evaluation of each major agency component (e.g. bureaus or operating divisions). OMB uses this data to distinguish good performing agency components from poor performers and to better focus oversight and assistance.

OMB’s reporting guidance also includes specific questions about individual FISMA requirements, including:

- Inventory of Systems. FISMA continues the Paperwork Reduction Act of 1995 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 agency programs to include security for information and information systems provided or managed by another agency, contractor, or other source. Thus, agencies must provide evaluations extending, as appropriate, beyond traditional agency boundaries.

- Implementation of security configurations. FISMA requires agencies to develop and implement minimally acceptable system configuration requirements. 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.[1]

B. OMB Circular A-11 “Preparation, Submission and Execution of the Budget”

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

[1] 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.

III. Government-wide Findings

A. Progress Against Government-wide Security Milestones

The Administration established three government-wide security goals in the 2004 President's budget:

- Goal 1 –More agencies must establish and maintain an agency-wide process for developing and implementing program and system level remediation plans. Plans of action and milestones must serve as an agency's authoritative management tool, to ensure program and system level IT security weaknesses, once identified, are tracked and corrected. By the end of 2003, all agencies should have an adequate process in place.

  Status – While each Federal agency now has a security remediation process, the effectiveness of those processes vary greatly. Out of 24 Federal agencies, IGs verified 18 as meeting OMB's criteria. OMB will continue to work with the remaining agencies to achieve this goal by the end of calendar year 2005.

- Goal 2 – By the end of 2003, 80% of Federal IT systems shall be certified and accredited.[2]

  Status – As of October 6, 2004, 77% of Federal information technology systems were certified and accredited. As the federal government works to achieve this goal, OMB has asked IGs to determine the quality of agency processes for certifying and accrediting systems. In particular, this will assure sufficient quality is achieved and agencies are following NIST guidance as we continue to make progress.

- Goal 3 – By the end of 2003, 80% of the Federal government's 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment.

[2] This goal and requirement derive from OMB policy found in Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 20, 1996, not FISMA. Sections 3a(4) and 3b(4) of Appendix III uses the term "authorize processing" to describe the certification and accreditation process. NIST Federal Information Processing Standard 102, September 1983, "Guideline for Computer Security Certification and Accreditation" provided detailed guidance on the process for unclassified systems, and was superseded in May 2004 by NIST Special Publication 800-37, "Guide for Security Certification and Accreditation of Federal Information Systems." Classified systems below the Sensitive Compartmented Information level are certified and accredited in accordance with NSTISSI 1000 "National Information Assurance Certification and Accreditation Process". Systems containing SCI information are certified and accredited in accordance with Director of Central Intelligence Directive 6/3 "Protecting Sensitive Compartmented Information within Information Systems".

Status – As of October 6, 2004, 85% of Federal information technology investments included security costs integrated into and funded over the lifecycle of the system's development and maintenance.

Below is a summary table showing progress in meeting these government-wide goals:

Table 1:
Overall Security Status and Progress from FY2002 to FY2004

	FY02	FY03	**FY04**
Goal 1: Number of Agencies and Percentage of Agencies with an IG Verified POA&M	Data Not collected in FY02	12 50%	**18** **75%**
Goal 2: Number of Systems and Percentage of Systems* with C&A	3772 47%	4969 62%	**6607** **77%**
Goal 3: Number of Systems and Percentage of Systems* with "Built-in" Security Costs	4919 62%	6182 77%	7295 **85%**

*Total number of systems reported: FY2002= 7957; FY03= 7998; FY2004= 8623. System count changes as agencies refine their system inventory and acquire, consolidate, or retire systems.

B. Agency Implementation of Key Security Performance Measures

Appendix A provides additional detail on Federal agencies' performance against key security performance measures. The tables within the appendix contain information from the agencies' FY 2004 FISMA reports.

C. Inspector General Assessment of Agency Plan of Action and Milestone Process

FISMA requires each agency 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. OMB's FISMA implementing guidance refers to this process as a security plan of action and milestones (POA&M).

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

OMB's FISMA reporting guidance requests that IGs assess whether their agency's POA&M process is adequate for the intended purpose. In FY 2003, IGs verified twelve agency processes met OMB's criteria. In FY 2004, the number rose modestly to eighteen. Table 2 below shows status in this area based on information provided agency IGs.

Table 2: Agency Inspector Generals were asked several questions to evaluate and verify whether the agency maintains and updates an effective plan of action and milestones (POA&M) process to remediate IT security weaknesses.

Agency	**Verified (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
Health and Human Services	No
Department of Homeland Security	No
Department of Housing and Urban Development	No
Department of Interior	Yes
Department of Justice	Yes
Department of Labor	Yes
National Aeronautics and Space Agency	Yes
National Science Foundation	Yes
Nuclear Regulatory Commission	Yes
Office of Personnel Management	Yes
Small Business Administration	No
Social Security Administration	Yes
State Department	Yes
Department of Transportation	Yes
Department of the Treasury	Yes
Department of Veterans Affairs	Yes
Total "Yes":	18
Total "No":	5

* DoD's IG provided information on The agency's POA&M process, however, unlike other agency IG submissions, the information was not consistent with what was requested in OMB reporting guidance.

D. Inspector General Assessment of Agency Certification and Accreditation process

Certification and accreditation of Federal information technology systems has been a policy requirement for several decades.[3] Certification is a comprehensive process of assessing the level of security risk, identifying security controls needed to reduce risk and maintain it at an acceptable level, documenting security controls in a security plan, and testing controls to ensure they operate as intended. Accreditation is a written decision by an agency management official authorizing operation of a particular information system (or group of systems). The decision is based upon a review of the certification documents and implementation of the agreed-upon set of security controls. In accrediting an information system, the agency official accepts responsibility and is accountable for continued adequate security of the system. Each system must be certified and accredited every three years, or whenever a significant change occurs to the system, whichever is sooner.

For the first time, in FY 2004, OMB requested IGs to review agency certification and accreditation processes and provide a qualitative assessment of this critical activity. As part of this assessment, IGs were asked to consider the degree to which the agency certification and accreditation process was consistent with NIST guidance.

Six IGs rated the agency certification and accreditation process as good, nine rated it as satisfactory and seven rated it as poor. None of the IGs rated the certification and accreditation process as failing. Table 3 below shows the outcome of the IGs assessment, listed by agency.

[3] *Id.*

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

Agency	**Evaluation**
Agency for International Development	Good
Department of Agriculture	Evaluation Incomplete
Department of Commerce	Poor
Department of Defense	Poor
Department of Education	Poor
Department of Energy	Satisfactory
Environmental Protection Agency	Satisfactory
General Services Administration	Good
Health and Human Services	Poor
Department of Homeland Security	Poor
Department of Housing and Urban Development	Poor
Department of Interior	Satisfactory
Department of Justice	Good
Department of Labor	Satisfactory
National Aeronautics and Space Agency	Poor
National Science Foundation	Good
Nuclear Regulatory Commission	Good
Office of Personnel Management	Satisfactory
Small Business Administration	Satisfactory
Social Security Administration	Satisfactory
State Department	Satisfactory
Department of Transportation	Satisfactory
Department of the Treasury	Good
Department of Veterans Affairs	Evaluation Incomplete
Total "Good":	6
Total "Satisfactory":	9
Total "Poor":	7
Total "Failing":	0
Total "Evaluation Incomplete":	2

E. OMB Assessment of Agency Incident Handling Programs

FISMA requires each agency to document and implement procedures for detecting, reporting and responding to security incidents. Agencies must also notify and consult with the Federal information security incident center operated by the Department of Homeland Security.[4] It also requires OMB oversight of the Federal information security incident center and NIST to issue incident detection and handling guidelines.[5]

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

In FY 2004, 2058 incidents were reported to the DHS incident response center. Based on consultation with DHS and the agencies, OMB is concerned with the accuracy, timeliness and completeness of incident reporting. DHS statistics indicate sporadic reporting by some agencies and unusually low levels of reported malicious activity at other agencies. 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, and thus complicates and delays appropriate response such as distributing security patches or other compensating controls.

In an effort to address this problem, DHS is piloting a tool for automatic transmittal of incident data from agency systems. This tool ensures privacy protection and should considerably improve the government's ability to protect systems and respond to attacks. OMB will continue to work with agencies and DHS to ensure appropriate processes and procedures are in place to prevent, prepare for, effectively respond to, and fully report on security incidents.

[4] 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.

[5] In January 2004, NIST published SP 800-61 "Computer Security Incident Handling Guide". 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. Per longstanding OMB policy, agencies must comply with NIST guidance.

IV. 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 red (agencies have any one of a number of serious flaws), yellow (agency has achieved intermediate levels of performance in all the criteria) or green (agency meets all the standards for success).

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 move forward, 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 Expanding E-Government Scorecard, agencies must meet the following three security criteria:

- Demonstrate consistent progress in remediation of security weaknesses
- Attain certification and accreditation of ninety percent of their operational systems, and,
- Maintain an IG assessed and verified agency POA&M process

In order to "maintain green," agencies must have by July 1, 2005:

- 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

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 scored on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

C. Security Line of Business

In FY 2005, OMB will work with the agencies to evaluate whether there is unnecessary duplication of resources used to achieve common government-wide security requirements. Consolidation of commonly used information technology security processes and technologies such as data collection and reporting, security patch management, and certification and accreditation tools may reduce costs and increase security consistency and effectiveness across government.

V. Conclusion

Over the past year, agencies made significant progress in closing the Federal government's information technology security performance gaps. Analysis of baseline performance measures indicates the following policy compliance improvements:

- 33% increase in the number of systems certified and accredited, from 4969 to 6607
- 18% increase in the number of systems with "built in" security costs, from 6182 to 7295
- 27% increase in the number of systems with tested security controls, from 5143 to 6515, and,
- 27% increase in the number of systems with tested contingency plans, from 3835 to 4886

However, uneven implementation of security measures across the Federal government leaves vulnerabilities to be corrected. OMB will use existing management processes to promote:

- Compliance with NIST publications including the new Federal Information Processing Standard (FIPS) 199 "Standards for Security Categorization of Information and Information Systems" and its companion document NIST Draft Special Publication 800-53 "Recommended Security Controls for Federal Information Systems"
- Implementation of FISMA requirements including security configuration guidance, completion of agency plans of action and milestones, development of contingency plans to recover information technology services following an emergency or system disruption, and methods used to ensure that contractor provided services are adequately secure, and,
- Quality improvement in agencies' system certification and accreditation processes

OMB's oversight of agencies' information technology security programs ensures FISMA requirements are met, and underscores the Director's commitment to strengthening the security of information technology systems, operations and assets.

VI. Additional Information

A. Appendix A: Individual Agency Summaries for the 24 CFO Act Agencies
B. Appendix B: Reporting by Small and Independent Agencies
C. Appendix C: Federal Government IT Security Program

Appendix A: Individual Agency Summaries for the 24 CFO Agencies

In FY 2004, all 24 CFO Act agencies submitted FISMA reports and a corresponding evaluation by the agency Inspector General or a designated independent assessor. See attached Excel Spreadsheet for individual agency performance metric summaries.

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

- Certification and Accreditation
- Integration of Security Control Costs into the System Lifecycle
- 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

Summary of Federal Government IT Security Performance Metrics

Total Number of systems	8623

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	77%
Security Costs Included in the System Lifecycle Costs:	85%
Tested Security Controls:	76%
Tested Contingency Plans:	57%
Percentage of Employees Trained in IT Security:	88%
Total IT Security Training Costs:	$55,001,002
Cost per employee trained:	$13.33

- Overall, configuration management policies for specific applications are being developed and implemented.
- Overall, incident management policies are being implemented.

Evaluation by the IG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes:	18 agencies
	No:	6 agencies
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes:	16 agencies
	No:	8 agencies
The agency maintains an inventory of major IT systems, updates it at least annually, and, the IG generally agrees with the contents of the inventory:	Yes:	15 agencies
	No:	9 agencies
Quality of agency C&A's:	Good:	6 agencies
	Satisfactory:	9 agencies
	Poor:	7 agencies
	Failing:	0 agencies
	Evaluation Incomplete:	2 agencies

Agency for International Development

Total Number of systems	9

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	100%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	100%
Tested Contingency Plans:	100%
Percentage of Employees Trained in IT Security:	99%
Cost per employee trained:	$69.82

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Good

· A system inventory is maintained and updated at least annually.
· The IG is not included in the development and verification of the system inventory, but, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of Agriculture

Total Number of systems	432

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	93%
Security Costs Included in the System Lifecycle Costs:	97%
Tested Security Controls:	94%
Tested Contingency Plans:	17%
Percentage of Employees Trained in IT Security:	68%
Cost per employee trained:	$8.19

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Evaluation Incomplete

· A system inventory is not consistently maintained.
· The IG is not included in the development and verification of a system inventory, and, the IG and CIO do not agree upon the number of systems, programs and contractor operations.

Department of Homeland Security

Total Number of systems	395

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	68%
Security Costs Included in the System Lifecycle Costs:	70%
Tested Security Controls:	76%
Tested Contingency Plans:	21%
Percentage of Employees Trained in IT Security:	85%
Cost per employee trained:	$43.64

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Poor

· A system inventory is not consistently maintained.
· The IG and CIO agree upon the number of systems, programs and contractor operations.

Department of Commerce

Total Number of systems	490

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	98%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	100%
Tested Contingency Plans:	92%
Percentage of Employees Trained in IT Security:	97%
Cost per employee trained:	$30.04

· Configuration management policies have not yet been developed and implemented.
· Incident management policies have not been fully implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Poor

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, however, the IG and CIO do not always agree upon the number of systems, programs and contractor operations.

Department of Defense

Total Number of systems	2213

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	58%*
Security Costs Included in the System Lifecycle Costs:	69%
Tested Security Controls:	35%
Tested Contingency Plans:	31%
Percentage of Employees Trained in IT Security:	88%
Cost per employee trained:	$9.33

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No**
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No**
Quality of agency C&A's:	Poor

· An accurate system inventory is not maintained, and the IG and CIO do not agree upon the number of systems, programs and contractor operations.

* Per Section 3543(c) of FISMA, the Secretary of Defense develops and oversees the implementation of policies on information security for DOD systems. DOD reports 58% of systems with approval to operate, and an additional 19% of systems with interim approval to operate.
** DoD's IG provided information on the agency's POA&M process, security of contractor provided services, and quality of C&A's separate from their annual report to OMB; however, unlike other agency IG submissions, the information was not consistent with what was requested in OMB reporting guidance.

Department of Energy

Total Number of systems	763

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	98%
Security Costs Included in the System Lifecycle Costs:	81%
Tested Security Controls:	85%
Tested Contingency Plans:	26%
Percentage of Employees Trained in IT Security:	96%
Cost per employee trained:	$26.42

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is not included in the development and verification of the system inventory, and, the IG and CIO do not agree upon the number of systems, programs and contractor operations.

Department of the Interior

Total Number of systems	157

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	83%
Security Costs Included in the System Lifecycle Costs:	98%
Tested Security Controls:	94%
Tested Contingency Plans:	66%
Percentage of Employees Trained in IT Security:	94%
Cost per employee trained:	$23.41

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained and updated at least annually.
· The IG is not included in the development and verification of the system inventory, but, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of Justice

Total Number of systems	198

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	91%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	100%
Tested Contingency Plans:	93%
Percentage of Employees Trained in IT Security:	91%
Cost per employee trained:	$18.91

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Good

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of Labor

Total Number of systems	85

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	96%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	91%
Tested Contingency Plans:	73%
Percentage of Employees Trained in IT Security:	99%
Cost per employee trained:	$26.74

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of Transportation

Total Number of systems	485

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	98%
Security Costs Included in the System Lifecycle Costs:	98%
Tested Security Controls:	98%
Tested Contingency Plans:	89%
Percentage of Employees Trained in IT Security:	98%
Cost per employee trained:	$7.94

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of Education

Total Number of systems	72

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	88%
Security Costs Included in the System Lifecycle Costs:	96%
Tested Security Controls:	93%
Tested Contingency Plans:	75%
Percentage of Employees Trained in IT Security:	80%
Cost per employee trained:	$18.63

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Poor

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Environmental Protection Agency

Total Number of systems	173

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	92%
Security Costs Included in the System Lifecycle Costs:	92%
Tested Security Controls:	90%
Tested Contingency Plans:	80%
Percentage of Employees Trained in IT Security:	90%
Cost per employee trained:	$22.68

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory. The IG and CIO agree upon the number of systems, programs and contractor operations.

General Services Administration

Total Number of systems	62

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	93%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	97%
Tested Contingency Plans:	62%
Percentage of Employees Trained in IT Security:	100%
Cost per employee trained:	$3.83

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Good

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, however, the IG and CIO do not always agree upon the number of systems, programs and contractor operations.

Department of Health and Human Services

Total Number of systems	172

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	97%
Security Costs Included in the System Lifecycle Costs:	90%
Tested Security Controls:	94%
Tested Contingency Plans:	30%
Percentage of Employees Trained in IT Security:	99%
Cost per employee trained:	$10.50

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented, however, HHS should strengthen internal reporting policies.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Poor

· A system inventory is maintained.
· The IG is not included in the development and verification of the system inventory, and, the IG and CIO do not always agree upon the number of systems, programs and contractor operations.

Department of Housing and Urban Development

Total Number of systems	187

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	24%
Security Costs Included in the System Lifecycle Costs:	28%
Tested Security Controls:	37%
Tested Contingency Plans:	1%
Percentage of Employees Trained in IT Security:	83%
Cost per employee trained:	$122.93

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Poor

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

National Aeronautics and Space Agency

Total Number of systems	1489

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	98%
Security Costs Included in the System Lifecycle Costs:	99%
Tested Security Controls:	95%
Tested Contingency Plans:	91%
Percentage of Employees Trained in IT Security:	100%
Cost per employee trained:	$22.40

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Poor

· A system inventory is maintained.
· The IG is not included in the development and verification of the system inventory, and, the IG and CIO do not agree upon the number of systems, programs and contractor operations.

Nuclear Regulatory Commission

Total Number of systems	17

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	100%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	94%
Tested Contingency Plans:	94%
Percentage of Employees Trained in IT Security:	87%
Cost per employee trained:	$15.32

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Good

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

National Science Foundation

Total Number of systems	21

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	90%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	90%
Tested Contingency Plans:	76%
Percentage of Employees Trained in IT Security:	96%
Cost per employee trained:	$18.60

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Good

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Office of Personnel Management

Total Number of systems	53

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	98%
Security Costs Included in the System Lifecycle Costs:	34%
Tested Security Controls:	94%
Tested Contingency Plans:	28%
Percentage of Employees Trained in IT Security:	100%
Cost per employee trained:	$9.98

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Small Business Administration

Total Number of systems	37

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	97%
Security Costs Included in the System Lifecycle Costs:	97%
Tested Security Controls:	62%
Tested Contingency Plans:	70%
Percentage of Employees Trained in IT Security:	97%
Cost per employee trained:	$9.88

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	No
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Social Security Administration

Total Number of systems	20

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	100%
Security Costs Included in the System Lifecycle Costs:	100%
Tested Security Controls:	100%
Tested Contingency Plans:	95%
Percentage of Employees Trained in IT Security:	100%
Cost per employee trained:	$9.25

- Configuration management policies for specific applications are being developed and implemented.
- Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Satisfactory

- A system inventory is maintained.
- The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

Department of State

Total Number of systems	178

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	92%
Security Costs Included in the System Lifecycle Costs:	88%
Tested Security Controls:	92%
Tested Contingency Plans:	92%
Percentage of Employees Trained in IT Security:	99%
Cost per employee trained:	$46.54

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Satisfactory

· A system inventory is not consistently maintained.
· The IG is not included in the development and verification of the system inventory, and, the IG and CIO do not agree upon the number of systems, programs and contractor operations.

Department of the Treasury

Total Number of systems	237

Metrics Reported by Agency CIO:

Effective Security and Privacy Controls (C&A):	86%
Security Costs Included in the System Lifecycle Costs:	95%
Tested Security Controls:	92%
Tested Contingency Plans:	66%
Percentage of Employees Trained in IT Security:	99%
Cost per employee trained:	$12.83

· Configuration management policies for specific applications are being developed and implemented.

· Incident management policies are being implemented.

Evaluation by the OIG:

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	No
Quality of agency C&A's:	Good

· A system inventory is maintained.

· The IG is not included in the development and verification of the system inventory, and, the IG and CIO do not agree upon the number of systems, programs and contractor operations.

Department of Veterans Affairs

Total Number of systems	678

<u>Metrics Reported by Agency CIO:</u>

Effective Security and Privacy Controls (C&A):	14%
Security Costs Included in the System Lifecycle Costs:	86%
Tested Security Controls:	83%
Tested Contingency Plans:	82%
Percentage of Employees Trained in IT Security:	77%
Cost per employee trained:	$12.77

· Configuration management policies for specific applications are being developed and implemented.
· Incident management policies are being implemented.

<u>Evaluation by the OIG:</u>

Process to Remediate IT Security Weaknesses is Verified (POA&M):	Yes
The agency has used appropriate methods to ensure that contractor provided services are adequately secure:	Yes
Quality of agency C&A's:	Evaluation Incomplete

· A system inventory is maintained.
· The IG is included in the development and verification of the system inventory, and, the IG and CIO generally agree upon the number of systems, programs and contractor operations.

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. Almost half of the small and independent agencies have regulatory or enforcement roles. The remaining half are largely 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. Altogether 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 2004, the Small Agency CIO Council worked with OMB to assist small agencies in complying with FISMA. In June 2004, the Council held a special FISMA workshop with small agency CIOs and IGs. The workshop featured speakers from OMB and NIST, and allowed individual agency IGs to discuss best practices for conducting FISMA reviews at small agencies. The Council also worked with OMB to develop streamlined FISMA reporting for micro-agencies to compensate for their smaller size and limited resources.

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.

In FY 2004, 57 small and independent agencies submitted FISMA reports. Of the 57 agencies submitting reports, 16 did not include an independent assessment meeting FISMA requirements.

This appendix contains an aggregated summary of reported performance metrics for those 57 agencies that submitted FISMA reports.

- Integration of Security Control Costs into the System Lifecycle. To date, 31 small and independent agencies have integrated their security control costs into the system lifecycle.

- Certification and Accreditation. Seventeen small and independent agencies have certified and accredited all of their systems. The lack of certification and accreditation at the 40 remaining small and independent agencies is a significant concern.

- Testing of Agency Security Controls. Twenty-five agencies reported they tested security controls annually for each of their systems. Thirteen agencies reported no such testing.

- Incident Handling Programs. Although almost all small and independent agencies have policies requiring incident reporting to DHS, some fail to characterize abnormal system activity as reportable incidents. In FY 2004, the small and independent agencies reported 195 incidents to DHS.

- Security Awareness, Training and Education. Agencies described 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. Twenty-two agencies reported they provided security training in FY 2004 for one hundred percent of their staff. Fourteen trained less than ten percent of their personnel. The remaining agencies reported their security education, training and awareness programs reached a moderate number of their workforce.

  For Employees with Significant Security Responsibilities. The agencies reported, on average, 61% of employees with significant security responsibilities received training in FY 2004. Specialized instruction was provided in practices such as network sniffer operation, firewall administration, and application software configuration.

- Contingency Planning. Although 29 agencies developed contingency plans for all of their IT systems, 7 agencies had done no contingency planning. The remaining agencies had prepared plans for selected systems.

  Testing. Contingency plans which are periodically tested are more viable than those not tested. Fourteen of the agencies serve as role models, having tested 100% of their contingency plans. In general, testing of contingency plans remains a concern, with only 34 agencies conducting any testing.

Small and Independent Agencies Submitting FISMA Reports in FY 2004

1. African Development Foundation
2. American Battle Monuments Commission
3. Appalachian Regional Commission
4. Barry Goldwater Scholarship and Excellence in Education Foundation
5. Broadcasting Board of Governors
6. Christopher Columbus Fellowship Foundation
7. Corporation for National and Community Service
8. Court Services and Offender Supervision Agency
9. Defense Nuclear Facilities Safety Board
10. Executive Office of the President, Office of Administration
11. Export/Import Bank of the United States
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 Labor Relations Authority
18. Federal Maritime Commission
19. Federal Reserve System
20. Federal Trade Commission
21. Inter-American Foundation
22. Institute of Museum and Library Services
23. Japan-US Friendship Commission
24. James Madison Memorial Fellowship Foundation
25. Millennium Challenge Corporation
26. Morris K. Udall Foundation
27. National Archives and Records Administration
28. National Credit Union Administration
29. National Endowment for the Arts
30. National Endowment for the Humanities
31. National Gallery of Art
32. National Labor Relations Board
33. National Mediation Board
34. Occupational Safety and Health Review Commission
35. Office of Federal Housing Enterprise Oversight
36. Office of Special Counsel
37. Overseas Private Investment Corporation
38. Peace Corps
39. Pension Benefit Guaranty Corporation
40. Postal Rate Commission
41. Railroad Retirement Board
42. Securities and Exchange Commission

43. Selective Service System
44. Smithsonian Institution
45. Tennessee Valley Authority
46. The Committee for Purchase from People who are Blind or Severely Disabled
47. U.S. Chemical Safety and Hazard Investigation Board
48. U.S. Commission of Fine Arts
49. U.S. Commodity Futures Trading Commission
50. U.S. Consumer Product Safety Commission
51. U.S. Equal Employment Opportunity Commission
52. U.S. Holocaust Memorial Museum
53. U.S. International Trade Commission
54. U.S. Merit Systems Protection Board
55. U.S. Nuclear Waste Technical Review Board
56. U.S. Trade and Development Agency
57. U.S. Office of Government Ethics

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 systems and national security systems. For both types of systems, the same management and evaluation requirements apply. The difference between the two programs is limited to policy setting authorities. For unclassified systems, OMB and NIST set policies and guidance. For national security systems, the interagency Committee on National Security Systems, established under National Security Directive 42 sets policies.

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.

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, DHS' Information Analysis and Infrastructure Protection Directorate provides government-wide assistance regarding intrusion detection and response, issues cyber alerts and warnings, 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, and 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 in the following ways:

- 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.

NIST's report can be found at: http://csrc.nist.gov/publications/nistir/IR7111-CSDAnnualReport.pdf The FY 2003 annual report highlights the publication of standards and guidelines which provide the foundation for strong information security programs at agencies. In addition, the report discusses NIST's outreach program to promote the understanding of IT security vulnerabilities and corrective measures.

In FY 2004, the Computer Security Division was actively engaged in the following activities:

- Publication of security guidelines. NIST published guidelines on a variety of topics. These included: certification and accreditation, incident handling, implementation of security controls, and standards for security categorization of Federal information systems.

  NIST has published the specific standards and guidelines mandated by FISMA. These are:

  - Special Publication 800-59 "Guideline for Identifying an Information System as a National Security System," August 2003
  - FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems," December 2003
  - Special Publication 800-61 "Computer Security Incident Handling Guide," January 2004
  - Special Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories," June 2004, and,
  - Special Publication 800-53 (Draft), "Recommended Security Controls for Federal Information Systems," January 2005

- Outreach activities. NIST conducts numerous outreach activities in order to assist agencies in implementing security guidelines. These outreach activities include presentations to the Federal Information Systems Security Educators' Association; leadership of the Federal Computer Security Program Managers' Forum, and management of the Program Review for Information Security Management Assistance.

- Common Criteria Project. NIST participates in the development of "Common Criteria" to evaluate information technology security. The security requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products. This work is undertaken in cooperation with NSA under NIST's National Information Assurance Partnership.

- Development of minimum security standards. NIST published the first public draft of *The NIST Security Configuration Checklists Program* in August 2004.

NIST's draft *Guidance for Securing Microsoft Windows XP Systems for IT Professionals* was published in July 2004.

- Security Research. NIST security research has continued in areas such as smart card specifications, quantum cryptographic-based protocols, approaches to more efficient and secure authorization techniques, as well as security of wireless and personal digital devices. NIST has also participated in the Critical Information Infrastructure Protection Working Group and provided input to the draft Federal Plan for Cyber Security Research and Development.

- Repository for Federal agency security practices. NIST hosts a growing repository of Federal Agency security practices, public/private security practices, and security configuration checklists for information technology products.

- Cryptographic Standards. NIST's Computer Security Division, in conjunction with the Government of Canada's Communications Security Establishment leads the Cryptographic Module Validation Program (CMVP). The Common Criteria Evaluation Validated Scheme (CCEVS) and CMVP facilitate security testing of information technology products useable by the Federal government.

- Coordination with the National Security Agency. NIST regularly engages with its counterparts in the national security community to help ensure a free flow of information, avoid duplication of effort and promote consistent approaches where appropriate and practicable. NIST officials participate as observers on the Committee for National Security Systems and national security officials also participate at meetings of NIST's Computer Security Program Managers' Forum. Under terms of a NIST-NSA Memorandum of Understanding, NSA and NIST jointly chair a Technical Working Group to support the development of cryptographic-based standards. Although developed and/or approved by NIST for unclassified systems, many of these have also been adopted for the protection of classified systems, under specific conditions, such as the Advanced Encryption Standard.

2. Assistance, Advice and Operations

Department of Homeland Security - DHS's National Cyber Security Division (NCSD) was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues and to coordinate the implementation of the President's *National Strategy to Secure Cyberspace*. In September 2003, NCSD created the United States Computer Emergency Readiness Team (US-CERT) as its operational component. US-CERT provides a national capability to link public and private response efforts, facilitates information sharing across all government agencies and infrastructure sectors, and helps protect and maintain the continuity of our Nation's cyber infrastructure.

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 2004, US-CERT issued twenty-two technical cyber security alerts regarding the presence of security vulnerabilities in commercial software. Agency officials were provided a description of the vulnerability, its impact, and the actions required to prevent exploitation of the weakness. US-CERT also issued seven Federal information bulletins warning agencies of specific threats from hackers and writers of malicious code. The information bulletins provided an assessment of the severity of the threat and recommended actions to limit exposure. Additionally, US-CERT published numerous cyber security bulletins and tips discussing security issues.

- 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 2004, agencies reported 2058 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.*

In FY 2005, OMB will continue to assist NCSD, including assistance in the drafting and publication of a "Concept of Operations for Federal Cyber Security Incident Handling" (CONOPS). The CONOPS will be a foundational document for NCSD, and will formally define US-CERT products and services available to its Federal customers. The CONOPS will be developed collaboratively with the agencies and will describe the inputs, processes and outputs of US-CERT.