Office of Management and Budget

FY 2003 Report to Congress on Federal Government Information Security Management

March 1, 2004

TABLE OF CONTENTS

I. Executive Summary

This report fulfills OMB's requirement under the Federal Information Security Management Act (FISMA) to submit an annual report to the Congress on agency compliance with IT security requirements in law and policy. FISMA directs Federal agencies to conduct annual IT security reviews and Inspectors General (IGs) to perform annual independent evaluations of agency programs and systems and report their results to OMB and Congress. To ensure consistent reporting across the government, OMB issued FISMA guidance, M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting", which included specific reporting instructions along with quantitative performance measures to more effectively determine agency status and progress. This guidance also continued the requirement for agencies to develop and manage a central plan of action and milestone (POA&M) process to prioritize and track IT security remediation efforts.

This report is based primarily on FY 2003 agency and IG reports to OMB, along with information provided through agency POA&Ms and OMB IT budget materials. The information and findings in this report do not include any actions undertaken after the submission of most agency and IG reports in September 2003.

The body of this report discusses the steps taken by OMB and Federal agencies to implement FISMA, details progress made in FY 2003, and identifies IT security gaps and weaknesses. Additionally, the report lays out a plan of action that OMB is pursuing with agencies throughout FY 2004 to close those gaps and improve the security of Federal information and systems. This plan of action aims to resolve information and security challenges through both management and budget processes.

Traditionally, OMB leverages management and budget processes to oversee and enforce agency information and system security remediation efforts. These processes enable OMB to hold agencies, including Chief Information Officers (CIOs) and agency program officials, accountable for the security of the information and systems that support their operations and assets. Specifically, OMB assesses and tracks progress through: 1) annual agency IT security reports and POA&Ms; 2) IT budget materials; 3) the President's Management Agenda under the E-Government Scorecard; 4) quarterly reports from agencies on their POA&M progress; and 5) quarterly updates from agencies on their progress against IT security performance measures.

Long-standing OMB policy requires agencies to incorporate IT security in the development of both new and existing IT investments and demonstrate that action in their IT budget materials. Agencies must: 1) report security costs for their IT investments; 2) document in their business cases that adequate security controls have been incorporated into the life cycle planning of each IT investment; 3) reflect the agency's security priorities as reported in their POA&Ms; and 4) tie their POA&Ms for an IT investment directly to the business case for that investment.

However, the central focus of this report is on performance accountability. In some areas this requires an acknowledgement of significant progress accomplished over the last three years. In other areas it requires a closer look and clearer understanding of the root cause for reoccurring weaknesses and the steps necessary to overcome them.

Finally, this report highlights government-wide milestones for improving information and system security that OMB initially identified and included in the President's FY 2004 budget and more recently updated in the President's 2005 budget.

Appendix A is a summary of the Federal government's IT security program, highlighting the roles and responsibilities of specific Federal agencies. Appendix B provides a brief summary of small and independent agency compliance with FISMA. Appendix C contains summaries for the 24 Chief Financial Officer (CFO) Act agencies.

A copy of this report is available at www.whitehouse.gov/omb. Additionally, OMB Circulars and guidance referenced in this report are also accessible at this website.

II. Introduction

A. IT Security Legislative History

The Government Information Security Reform Act of 2000 (GISRA) brought together existing IT security requirements in previous legislation, namely the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Reform Act of 1996 (Clinger-Cohen). GISRA also codified existing OMB IT security policies found in OMB Circular A-130, "Management of Federal Information Resources" and OMB IT security budget guidance in Circular A-11, "Preparation, Submission, and Execution of the Budget".

Additionally, GISRA introduced annual review and reporting requirements for agencies and IGs. Specifically, GISRA directed agency CIOs to conduct annual IT security reviews of their systems and programs. Agency program officials were also required to annually review all of the systems that support their programs. Additionally, agency IGs must perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews and evaluations are reported annually to OMB and are the basis of this report.

Fundamentally, GISRA recognized that while security clearly has a technical component, it is at its core an essential management function. Additionally, GISRA brought forward a much needed emphasis on accountability. In particular, while agency CIOs have an agency-wide leadership role, agency program officials are ultimately responsible for ensuring the security of the information and systems that support their operations and assets.

After GISRA expired in November 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. Title III of that Act, FISMA, permanently reauthorized the framework laid out in GISRA. The enactment of FISMA was a critical step that ensured the continuation of GISRA requirements and therefore the ability to effectively identify and track the Federal government's information and system security status. FISMA also includes new provisions aimed at further strengthening information and system security. In particular, FISMA directs the National Institute of Standards and Technology (NIST) to develop IT security guidelines in a number of key areas such as developing minimum security standards for agency systems. NIST has been actively working with agencies in the development of those standards per their statutory role in providing technical guidance to Federal agencies. Additional detail on NIST's activities is provided in Appendix A.

Below are some of the other changes or additions introduced by FISMA:

- Broadening the applicability of security requirements to include information and information systems. Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has

somewhat broader applicability than that of prior security law. That is, agency IT security programs apply to all organizations or sources which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. FISMA therefore underscores longstanding OMB policy concerning sharing government information and interconnecting systems, i.e., Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

- Stronger emphasis on configuration management. FISMA requires each agency to develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.

- Codifies requirement for ensuring continuity of system operations. FISMA codifies a longstanding policy requirement that each agency's security program (and particularly each system security plan) include the provision for the continuity of operations for information systems that support the operations and assets of the agency. FISMA explicitly includes in this requirement, information and information systems "provided or managed by another agency, contractor, or other source."

- Development and maintenance of an inventory of major information systems. FISMA amends the Paperwork Reduction Act regarding the major information systems (including major national security systems) operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of "major information system" is found in OMB Circular A-130.

  The FISMA amendments requires that the identification of information systems in this inventory include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. OMB's guidance directed agencies to leverage their enterprise architecture work to create this inventory.

B. Purpose and Scope of Annual IT Security Report

This report provides a government-wide assessment of IT security strengths and challenges, individual summaries of agency performance, and a plan of action for next steps to successfully resolve weaknesses and continue to improve the Federal government's overall IT security posture. Additionally, this report examines agency status against key IT security performance measures from FY 2001 through FY 2003.

The agency summaries in Appendix C are based solely on agency and IG work conducted in FY 2003 and do not include any efforts undertaken after September 2003. However, since completion of their FY 2003 reviews, agencies have been working to prioritize their IT security weaknesses and developing and implementing program and system level plans of action and milestones (POA&Ms) to remediate those weaknesses.

III. OMB IT Security Guidance

A. Reporting Instructions and Measuring Performance

In August 2003, OMB provided instructions for Federal agencies' reporting the results of their annual reviews and evaluations. This guidance highlighted changes introduced by FISMA from GISRA. The specific reporting instructions for agencies and IGs remained nearly identical to FY 2002 and were mapped directly to the requirements in FISMA. As a result, status against the FY 2001 baseline (both improvements and weaknesses) is easily identifiable.

Other key requirements in OMB's FISMA guidance include:

- Continuation of IT security performance measures. Agencies and IGs were directed to report the results of their work against a key set of IT security performance measures. These measures have proved extremely valuable in identifying agency strengths and weaknesses, prioritizing resource decisions, and assisting OMB in our oversight activities. A table of agency performance against the IT security measures from FY 2001 through FY 2003 can be found on page 10.

- Continuation of IT security remediation efforts. OMB guidance continued the requirement that Federal agencies develop POA&Ms for every program and system where an IT security weakness has been found. POA&Ms must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, identified by the agency, IG, GAO, or OMB, are tracked and corrected. These plans must be developed, implemented, and managed by the agency official who owns the program or system (either an agency program official or the agency CIO depending on the system) where the weakness was found. System-level POA&Ms must also be tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11). This is an important step that ties the justification for IT security funds to the budget process.

  To ensure successful remediation of security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor agency remediation efforts. OMB's FY 2003 FISMA reporting instructions requested IGs to assess whether or not an agency has a process in place that meets criteria laid out in OMB guidance.

B. Budgeting for IT Security

Long-standing OMB policy requires agencies to ensure that security is addressed throughout the budget process. Agencies are directed to: 1) report security costs for their IT investments; 2) document in their business cases that adequate security controls have been incorporated into the life cycle planning of each IT investment; 3) reflect the agency's security priorities as reported in their POA&Ms; and 4) tie their POA&Ms for an IT investment directly to the business case for that investment.

Security must be incorporated into the life-cycle of every IT investment. To identify the appropriate security controls, agencies must first assess the risks to their information and systems. As part of the IT business case requesting funds for major systems, agencies report on the risk assessment as well as their compliance with security requirements, such as the development of security plans and certification and accreditation. Failure to appropriately incorporate security in new and existing IT investment puts the investment at considerable risk for funding. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems that have an out-of-date certification and accreditation.

Funding for IT security has increased from $2.7 billion in FY 2002 to $4.2 billion in FY 2003. Historically, a review of IT security spending and security results has demonstrated that spending is not a statistically significant factor in determining agency security performance. Rather, the key is effectively incorporating IT security in agency management actions and implementing IT security throughout the lifecycle of a system.

IV. OMB's Government-wide Findings

A. Progress Against Government-wide IT Security Milestones

OMB established three government-wide goals in the President's FY 2004 Budget and recently provided an update against these measures in the President's FY 2005 Budget:

- Goal 1 – By the end of calendar year 2003, all Federal agencies will have created a central remediation process to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected. Each agency IG will verify whether or not the agency has a process in place that meets criteria laid out in OMB guidance.

  Status – While each Federal agency does have an IT security remediation process, the maturity of those processes vary greatly. Out of the twenty-four CFO Act agencies, twelve agencies have a remediation process verified by their IG as meeting the necessary criteria. OMB will continue to work with the remaining Federal agencies to achieve the full goal in 2004.

- Goal 2 – By the end of calendar year 2003, 80 percent of Federal IT systems shall be certified and accredited. Many agencies are not adequately prioritizing their IT

investments to ensure that significant IT security weaknesses are appropriately addressed.

Status – At the end of 2002, nearly 47% of Federal IT systems had been certified and accredited. This percentage increased to 62% at the end of 2003.

- Goal 3 – By the end of calendar year 2003, 80 percent of the Federal government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment. While agencies have made improvements in integrating security into new IT investments, significant problems remain, particularly in ensuring security of existing systems.

  Status – At the end of 2002, over 60% of Federal IT systems planned and budgeted for IT security requirements as part of the overall development or maintenance of systems. This percentage increased to 78% at the end of 2003.

B. Agency Progress Against Key IT Security Performance Measures

Agencies' FY 2001 reports established a baseline of agency IT security performance. To ensure that progress could be consistently determined against that baseline, the FY 2002 reporting instructions remained nearly identical to the FY 2001 requirements. For the first time, as a result of GISRA requirements and OMB performance measures, the Federal government is able to measure progress in IT security. Federal agencies, OMB, the Congress, and the General Accounting Office (GAO) are able to track and monitor agency efforts using those measures. While the Federal government is heading in the right direction additional efforts are still warranted. For example, there are notable increases in the percentage of systems with security plans and the percentage of systems certified and accredited. However, many Federal systems do not have appropriate contingency plans in place to ensure continuity of operations. Another continuing area of concern is the low government-wide percentage of system with tested contingency plans. Table 1 below provides a summary of Federal agencies' performance against these key IT security measures from FY 2001 through FY 2003. Please note that this table contains information as it was reported in agencies' FY 2002 and FY 2003 FISMA reports. When reviewing this information, it is also important to recognize that the total number of agency systems tends to change from FY 2001 to FY 2003. A goal of the FY 2004 OMB FISMA guidance is to standardize more of the annual reporting, including clearer definitions to eliminate interpretation differences.

Table 1. FY 2001, FY 2002, and FY 2003 IT Security Status and Progress by Agency

Agency	Total No. and % of Systems			No. and % of systems assessed for risk and assigned a level of risk			No. and % of systems that have an up-to-date IT security plan			No. and % of systems authorized for processing following certification and accreditation			No. and % of systems with security control costs integrated into the life cycle of the system			No. and % of systems for which security controls have been tested and evaluated in the last year			No. and % of systems with a contingency plan			No. and % of systems for which contingency plans have been tested		
	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03
AID	89	89	8	28	85	7	12	63	7	10	89	7	5	20	8	15	75	1	13	38	1	1	3	0
				31%	96%	88%	13%	71%	88%	11%	100%	88%	6%	22%	100%	17%	84%	13%	15%	43%	13%	1%	3%	0%
USDA	580	605	271	59	111	196	325	142	182	42	46	37	146	156	249	105	125	83	136	143	155	65	62	79
				10%	18%	72%	56%	23%	67%	7%	8%	14%	25%	26%	92%	18%	21%	31%	23%	24%	57%	11%	10%	29%
DOC	646	609	555	475	571	555	447	584	555	311	467	541	542	520	495	438	521	502	347	493	549	61	83	421
				74%	94%	100%	69%	96%	100%	48%	77%	97%	84%	85%	89%	68%	86%	90%	54%	81%	99%	9%	14%	76%
DOD	155	155	378	125	106	343	130	103	334	95	85	302	48	62	242	35	43	157	131	103	299	33	32	191
				81%	68%	91%	84%	66%	88%	61%	55%	80%	31%	40%	64%	23%	28%	42%	85%	66%	79%	21%	21%	51%
ED	57	92	76	42	92	76	22	36	69	0	0	10	0	0	11	38	49	75	32	40	36	14	37	68
				74%	100%	100%	39%	39%	91%	0%	0%	13%	0%	0%	14%	67%	53%	99%	56%	43%	47%	25%	40%	89%
DOE	961	906	1172	587	597	1041	719	720	1075	205	420	970	468	488	1112	532	554	1014	203	221	792	130	148	316
				61%	66%	89%	75%	79%	92%	21%	46%	83%	49%	54%	95%	55%	61%	87%	21%	24%	68%	14%	16%	27%
EPA	189	168	164	174	168	164	168	156	154	172	146	154		129	141	87	107	144		94	132		31	49
				92%	100%	100%	89%	93%	94%	91%	87%	94%		77%	86%	46%	64%	88%		56%	80%		18%	30%
GSA	42	56	67		20	37	26	29	37	6	7	15	39	22	56	1	7	39		21	30		12	21
					36%	55%	62%	52%	66%	14%	13%	27%	93%	39%	100%	2%	13%	70%		38%	54%		21%	38%
HHS	277	283	222	21	122	153	38	107	177	10	31	90	136	230	194	45	95	138	40	93	107	15	44	60
				8%	43%	69%	14%	38%	80%	4%	11%	41%	49%	81%	87%	16%	34%	62%	14%	33%	48%	5%	16%	27%
DHS			346			147			155			145			152			65			123			44
						42%			45%			42%			44%			19%			36%			13%
HUD	48	127	197	42	119	17	46	107	17	41	92	17	44	99	197	41	97	14	48	127	197	48	127	0
				88%	94%	9%	96%	84%	9%	85%	72%	9%	92%	78%	100%	85%	76%	7%	100%	100%	100%	100%	100%	0%
DOI	224	224	164	27	42	71	34	70	87	18	49	17	65	109	158	26	51	99	36	63	56	17	23	32
				12%	19%	43%	15%	31%	53%	8%	22%	10%	29%	49%	96%	12%	23%	60%	16%	28%	34%	8%	10%	20%
DOJ	235	275	255	194	210	229	157	196	220	194	209	202	118	148	220	128	143	197	91	117	196	18	29	80
				83%	76%	90%	67%	71%	86%	83%	76%	79%	50%	54%	86%	54%	52%	77%	39%	43%	77%	8%	11%	31%
DOL	52	46	81	49	45	75	49	44	77	15	32	47	42	41	72	38	42	59	47	46	75	14	14	36
				94%	98%	93%	94%	96%	95%	29%	70%	58%	81%	89%	89%	73%	91%	73%	90%	100%	93%	27%	30%	44%
NASA	1694	1641	1555	183	1641	1516	183	1489	1297	183	1459	1520	183	1641	1547	183	1600	1292	162	1600	1471	152	1453	1302
				11%	100%	97%	11%	91%	83%	11%	89%	98%	11%	100%	99%	11%	98%	83%	10%	98%	95%	9%	89%	84%
NSF	15	20	19	12	20	19	10	18	18	0	6	18	15	20	19	6	20	18	6	11	16	6	9	15
				80%	100%	100%	67%	90%	95%	0%	30%	95%	100%	100%	100%	40%	100%	95%	40%	55%	84%	40%	45%	79%
NRC	23	18	20	2	18	20	2	18	18	2	9	18	15	18	20	2	10	18	2	13	18	0	7	17
				9%	100%	100%	9%	100%	90%	9%	50%	90%	65%	100%	100%	9%	56%	90%	9%	72%	90%	0%	39%	85%
OPM		42	45		5	41		4	41		0	41		0	18		9	41		6	16		6	7
					12%	91%		10%	91%		0%	91%		0%	40%		21%	91%		14%	36%		14%	16%
SBA	37	37	38	14	22	28	15	22	28	14	24	28	0	5	5	0	2	7	7	7	15	7	7	15
				38%	59%	74%	41%	59%	74%	38%	65%	74%	0%	14%	13%	0%		18%	19%	19%	39%	19%	19%	39%

Agency	Total No. and % of Systems			No. and % of systems assessed for risk and assigned a level of risk			No. and % of systems that have an up-to-date IT security plan			No. and % of systems authorized for processing following certification and accreditation			No. and % of systems with security control costs integrated into the life cycle of the system			No. and % of systems for which security controls have been tested and evaluated in the last year			No. and % of systems with a contingency plan			No. and % of systems for which contingency plans have been tested		
	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03
SSA	16	17	17	16	17	17	16	17	17	16	17	17	16	17	17	16	17	17	16	17	16	15	16	14
				100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	94%	94%	94%	82%
State		344	139		256	139		53	51		0	50		30			189	46		38	41		0	50
					74%	100%		15%	37%		0%	36%		9%			55%	33%		11%	29%		0%	36%
DOT	427	677	630	220	85	378	113	97	286	111	56	209	102	110	415	146	100	328	119	114	167	43	49	103
				52%	13%	60%	26%	14%	45%	26%	8%	33%	24%	16%	66%	34%	15%	52%	28%	17%	27%	10%	7%	16%
TREAS	598	624	708	343	258	304	131	261	304	101	266	172	355	486	203	302	418	156	233	326	315	53	77	291
				57%	41%	43%	22%	42%	43%	17%	43%	24%	59%	78%	29%	51%	67%	22%	39%	52%	44%	9%	12%	41%
VA	995	851	871	582	542	663	330	581	632	407	262	342	662	563	631	263	469	633	547	603	627	536	499	628
				58%	64%	76%	33%	68%	73%	41%	31%	39%	67%	66%	72%	26%	55%	73%	55%	71%	72%	54%	59%	72%
TOTAL	7360	7906	7998	3195	5152	6236	2973	4917	5838	1953	3772	4969	3001	4914	6182	2447	4743	5143	2216	4334	5450	1228	2768	3839
TOTAL				43%	65%	78%	40%	62%	73%	27%	48%	62%	41%	62%	77%	33%	60%	64%	30%	55%	68%	17%	35%	48%

C. IGs Assessment of Agency Plan of Action and Milestone Process

FISMA, along with OMB's implementing guidance directs agencies to develop and implement POA&Ms for all systems with weaknesses. To ensure that remediation plans continue to be developed and implemented, and corrective actions prioritized and tracked, each agency must put in place a robust agency-wide plan of action and milestone process. OMB's FY 2003 FISMA guidance, requested IGs to assess against a set of criteria whether such a process exists. Table 2 below details each agency IG's response. OMB emphasizes the importance of an IG verified process by including it as one of three criteria necessary for agencies to "get to green" for IT security on the Expanding E-Government Scorecard of the President's Management Agenda. Please note that this table contains information as it was reported in IGs' FY 2003 FISMA reports.

Table 2. IG Assessment of Agency Plan of Action and Milestone (POA&M) Process

Agency	IG Assessment of Whether Agency POA&M Process Meets Minimum Criteria in OMB FISMA Guidance
Agency for International Development	Yes
Agriculture	No
Commerce	Yes, but process will need to better tie system-level POA&Ms to budget request for that system.
Defense	Have not received DOD IG Report
Education	Yes
Energy	Yes, but process will need to better tie system-level POA&Ms to budget request for that system.
Environmental Protection Agency	Yes, but process will need to improve prioritization efforts.
General Services Administration	No
Health and Human Services	No
Homeland Security	No
Housing and Urban Development	No
Interior	No
Justice	No
Labor	Yes
National Aeronautics and Space Administration	No
National Science Foundation	Yes
Nuclear Regulatory Commission	Yes
Office of Personnel Management	Yes
Small Business Administration	No
Social Security Administration	No
State	Yes
Transportation	Yes
Treasury	No
Veterans Affairs	Yes, but need to take additional steps to allow IG access to POA&M process.

D. Lack of Clear Accountability for Ensuring Security of Information and Systems

Even with the strong focus of both GISRA and FISMA on the responsibilities of agency officials regarding security, there continues to be a lack of understanding and therefore accountability within the Federal government. In the FY 2002 GISRA report, OMB identified a number of troubling government-wide issues and trends. Some of those issues continue to be of concern and are listed below.

- Agency and IG reports continue to identify the same IT security weaknesses year after year, some of which are seen as repeating material weaknesses.
- Additionally, while the Federal government appears to be doing a much better job at planning for the security of new IT investments, too many legacy systems continue to operate with serious weaknesses.
- As a result, there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development.

While there are a number of options available to address these concerns they must ultimately be addressed through improved accountability. Even though awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. Ensuring the security of most agency information and systems is not the responsibility of the agency CIO. The majority of IT spending within agencies is not on IT infrastructure and networks, traditionally owned and operated by CIOs, but rather on mission IT investments. In fact, historically, over 65% of agency IT investments are normally mission-IT related. It is within these systems that many weaknesses recur.

Law and policy are clear; IT security is not the responsibility of a single agency official or the agency's IT security office. It is a shared responsibility and holding just one official accountable potentially weakens an agency's ability to properly safeguard its entire collection of IT investments.

Through the President's Management Agenda, OMB has increased accountability for agency security performance; however, greater consistency within agencies is necessary.

V. Plan of Action to Improve Performance

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains to improve the security of the information and systems that support the Federal government's missions. To address existing and new challenges, and continue improvements, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets. Throughout all of these steps OMB will be reviewing options to increase accountability.

Specifically, OMB will pursue the steps outlined below as a plan of action to both assist agencies in their IT security efforts, promote implementation of law and policy, as well as track status and progress.

A. Prioritizing IT Spending to Resolve IT Security Weaknesses

Long-standing OMB policy directs agencies to fund IT security throughout the life cycle of every system and develop remediation plans for all systems with IT security weaknesses.

OMB used the information from the annual FISMA reports and quarterly remediation updates to directly inform the FY 2005 budget process. Specifically:

- Information from agency and IG reports along with their remediation plans identified both agency-wide and system specific IT security weaknesses. The annual reviews and reports identified the gaps and the remediation plans provide the corrective actions the agency has determined will close the gaps. This appears equally true for national critical assets and mission critical systems.

- Information from IT budget documents, such as the exhibit 53 and 300, also identify whether appropriate steps to secure both new and legacy IT investments have been undertaken. For example, agencies must report whether risk-based and cost-effective IT security controls have been identified, implemented, and tested and their operational systems have been fully certified and accredited.

While this information assisted OMB in making FY 2005 funding decisions, thereby addressing longer-term IT security weaknesses, it was also useful in prioritizing FY 2004 funding decisions. For example, agencies with significant information and system security weaknesses were directed to remediate operational systems with weaknesses prior to spending FY 2004 IT development or modernization funds. If additional resources are needed to resolve those weaknesses, agencies are to use those FY 2004 IT funds originally sought for new development. These steps were taken to reinforce both law and policy requirements and they underscore the President's commitment to security and privacy.

B. President’s Management Agenda Scorecard

Outside of OMB’s annual conditional approval or disapproval of agency information security programs, the President’s Management Agenda Scorecard is one of the most important mechanisms for both acknowledging agency IT security progress and highlighting significant problems. OMB uses all of the agency IT security materials to help inform the quarterly assessment of the scorecard.

To “get to green” under the Expanding E-Government Scorecard for IT security, agencies must meet the following three criteria: 1) demonstrate consistent progress in remediating IT security weaknesses; 2) attain certification and accreditations for 90% of their

operational IT systems; and 3) IG assessed and verified agency POA&M process. Only a sound institutionalized remediation process will support consistent IT security improvements. OMB will continue to assess each quarter agency remediation efforts.

In addition to receiving updates on agency performance against key IT security performance measures, beginning in December 2003, agencies started reporting each quarter on their status against a subset of those measures. These quarterly updates are sent to OMB along with agencies quarterly updates on their POA&M efforts and are used to inform the quarterly assessment of the President's Management Agenda Scorecard.

C. FY 2004 OMB FISMA Guidance

As we progress into the fourth year of these annual IT security requirements, our goal is to move even more toward performance measurement. The ability to clearly determine outcomes and results is essential. Therefore, it is critically important that FISMA reporting instructions mature to focus on the key IT security areas and collect the most useful information to inform agencies, OMB, and the Congress on the status of agency efforts to secure their systems and protect their information. In particular, as part of the development of OMB's FY 2004 FISMA guidance, we are focusing on the following three areas: 1) evolving the IT security performance measures to move further beyond status reporting to also identify the quality of the work done. For example, being able to determine both the number of systems certified and accredited as well as the quality of the certification and accreditation conducted; 2) the independent evaluations by the IGs continue to be a source of indispensable information and further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes such as remediation and intrusion detection and reporting are invaluable; and 3) providing additional clarity to certain definitions to eliminate interpretation differences within agencies and between agencies and IGs.

D. Threat and Vulnerability Response Process

While the Federal government has focused increased attention and resources to securing our information and systems, resulting in more rigorous evaluations, new threats and vulnerabilities continue to materialize. Therefore, we must continue to improve the Federal government's incident prevention and management capabilities. Such improvements include an increased emphasis on reducing the impacts of worms and viruses through more timely installation of patches for known vulnerabilities, and improved information sharing to rapidly identify and respond to cyber threats and critical vulnerabilities. Already these steps have led to stronger government-wide processes for intrusion detection and response, significantly diminishing the potential impacts of many recent worms and viruses. It is virtually impossible to ensure perfect security of IT systems and the increasing number and potential impact of threats and vulnerabilities underscores the critical importance for agencies to maintain business continuity plans.

Additionally, DHS created the National Cyber Security Division within the Information Analysis and Infrastructure Protection Directorate to improve the Federal government's

response to cyber attacks and vulnerabilities. Integrating FedCIRC, the National Infrastructure Protection Center (NIPC), the National Communications System (NCS), and the CIAO under the Information Analysis and Infrastructure Protection Directorate of DHS, and partnering with the Science and Technology directorate on research and development needs, consolidates expertise and resources, increases efficiency, and presents an opportunity for the Administration to strengthen government-wide processes for incident prevention, detection and response and improve critical infrastructure protection. Additional information on DHS' responsibilities in this area is provided in Appendix A.

VI. Conclusion

Ensuring the security of the information and systems that support the Federal government's operations and assets has been a shared priority for the Administration and Congress for many years. Due to the annual reporting requirements first introduced by GISRA and continued by FISMA, the Federal government now has three years of data to assess status and progress, identify strengths and weaknesses, and focus on areas of greatest need, thereby promoting wiser IT investments.

While the Federal government has made significant strides in identifying and addressing long-standing problems, agency and IG reports reveal that challenging weaknesses remain.

Like GISRA, FISMA has been instrumental in improving the state of Federal IT security, both the security of systems and promoting the protection of information. We acknowledge the agencies and IGs for their significant work and identifiable progress since FY 2001. OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets, while enabling and not unnecessarily impeding the government's missions.

VII. Additional Information

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

Appendix A: Federal Government's IT Security Program

The Federal government's IT security program is divided between security for unclassified information and systems and national security information and systems. The information below focuses on the Federal government's IT security program for unclassified information and systems which is based in statute. Applicable laws include:

- The Computer Security Act[1] expressly separated classified programs from unclassified programs, gave the National Institute of Standards and Technology (NIST) the responsibility to develop security standards and guidelines for sensitive but unclassified Federal information and systems, and required agencies to prepare security plans and conduct training.

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

- 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 (FISMA), title III of the Electronic Government Act, reauthorizes the provisions found in the Government Information Security Reform Act which expired in November 2002. FISMA generally codifies OMB's security policies and continues the same framework established by the foregoing statutes while requiring annual agency program and system reviews, independent IG evaluations, annual agency reports to OMB, and an annual OMB report to Congress. At the policy level, FISMA maintains the separation between unclassified programs and national security programs. Additionally, FISMA emphasizes accountability for agency officials' security responsibilities, e.g., the role of agency program officials in ensuring that the systems that support their operations and assets are appropriately secure.

<u>Federal Agencies with Specific IT Security Responsibilities</u>

Federal agencies with IT security responsibilities can be divided into two areas – those with policy and guidance authorities and those with assistance, advice, and operational authorities. For the Federal government's unclassified IT security program, OMB and NIST issue policy and guidance. In the area of assistance, advice, and operations, the Department of Homeland Security (DHS) under the Information Analysis and Infrastructure Protection Directorate provides government-wide assistance regarding intrusion detection and response, issues cyber alerts and warnings, as well as partners with other agencies, industry, academia, and state and local governments and organizations to identify and protect our nation's critical cyber operations and assets.

[1] The Computer Security of 1987 was repealed by the Federal Information Security Management Act of 2002.

Listed below are the agencies with specific responsibilities that support the Federal government's IT security program.

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 IT security program.

Within this statutory framework, OMB issues IT security policies (e.g., OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" and OMB budget guidance, Circular A-11) and NIST issues technical guidance (via Federal Information Processing Standards and Special Publications). NIST developed technical guidelines assists agencies in implementing law and OMB policy. OMB oversight and enforcement is achieved largely in the following ways:

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

OMB fulfills its role through the Office of E-Government, working with the Office of Information and Regulatory Affairs. The key to effective OMB oversight of agency IT security is performance review and assessment by OMB's many professional management and budget staff. This is an ongoing activity through the President's Management Agenda Scorecard and budget processes.

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 and systems. OMB policy requires that agency security programs and practices be consistent with NIST guidance. NIST IT security standards and guidelines are a significant part of the Federal government's IT security program and continue to introduce consistency and discipline. NIST performs its statutory responsibilities through the Computer Security Division of the Information Technology Laboratory.

As part of the annual report to Congress, OMB is directed to include a summary of and the views of the Director on NIST's "annual public report on activities undertaken in the previous year and planned for the coming year." As of the date of this report, NIST's report is under development so OMB is unable to provide comments at this time. However, a list of a number of NIST activities is provided below.

FISMA charges NIST with developing and issuing IT security guidelines in a number of key areas such as developing minimum security standards for agency systems. NIST has been actively working with agencies in the development of those standards. Additionally, agencies are required to implement NIST standards and OMB will continue to direct agency use of NIST IT security guidelines.

NIST is currently engaged in a number of IT security initiatives:

- Providing management and assistance (e.g., certification and accreditation of systems, procurement guidelines, security and capital planning guidelines, self-assessment tools).
- Drafting and publishing numerous security guidelines covering a wide variety of topics such as email, firewalls, telecommuting and contingency planning. A number of draft guidelines are now being reviewed by Federal agencies and other interested parties concerning such topics as certification and accreditation, awareness and training, and considerations for Federal IT procurement.
- Developing minimum security standards as required by FISMA.
- Maintaining the "Common Criteria" which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with NSA under NIST's National Information Assurance Partnership.
- Conducting security research (e.g., access control, wireless, mobile agents, smart-cards, quantum computing).
- Operating a computer security expert assist team (CSEAT) to assist Federal agencies in identifying and resolving IT security problems.
- Maintaining a website of effective Federal agency security practices which share proven successes across the Federal government. This website will be expanded to include private sector practices as required by FISMA.
- Continuing Crypto standards, Cryptographic key management, Smart card security, and E-authentication work.

2. Assistance, Advice and Operations:

Department of Homeland Security. The following previously separate offices and their functions were transferred in March 2003 to DHS under their Information Analysis and Infrastructure Protection (IAIP) Directorate.

- The Federal Computer Incident Response Center (FedCIRC), formerly at the General Services Administration, assists agencies in responding to computer security incidents

and coordinating cross-agency sharing of information on common vulnerabilities. FedCIRC provides agencies with technical information, tools, methods, assistance, and guidance.

- The National Infrastructure Protection Center (NIPC), formerly of the Department of Justice, investigates crimes related to unauthorized intrusions into U.S. Government and commercial sites. In addition, it served as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services.

- The Critical Infrastructure Assurance Office (CIAO), formerly of the DOC, assists agencies in identifying and prioritizing critical assets and system interdependencies. The office also performs an outreach to industry not directly related to the government IT security program.

Integrating these offices and their functions under the IAIP Directorate of DHS, consolidates expertise and resources, increases efficiency, and strengthens government-wide processes for incident prevention, detection, and response and improves critical infrastructure protection. In FY 2003, DHS created within the IAIP Directorate a cyber security division. This division provides 24 x 7 functions, including performing analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts.

Below are the initial initiatives that the division is addressing:

- Identify risks and help reduce the vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets;
- Oversee a consolidated Cyber Security Tracking, Analysis, & Response Center (CSTARC), which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cyber security and incident response with federal, state, local, private sector and international partners; and
- Create, in coordination with other appropriate agencies, cyber security awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.

FISMA charges the Director of OMB with oversight of FedCIRC. In accordance with FISMA, the center has the following primary functions:

- Providing agencies with information regarding information security threats and vulnerabilities

  In FY03, FedCIRC issued 35 advisories alerting agencies to 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. If the risk to government systems was deemed to be particularly high, agencies were asked to confirm with OMB that corrective action had been taken.

The implementation of the countermeasures identified in the FedCIRC advisories successfully limited the effect of Internet exploits such as the Blaster and Sobig worms on government systems.

In FY03, FedCIRC also issued 15 informational notices warning agencies of specific threats from hackers and writers of malicious code. The informational notices provided an assessment of the severity of the threat and recommended actions to limit exposure.

- Analysis of incidents that threaten information security

  In order to comprehensively examine cybersecurity incidents, FedCIRC 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.

  Although 506,291 incidents were reported to FedCIRC in FY03, OMB has a continuing concern regarding the timeliness and accuracy of reporting of incidents by agencies. Although agencies are aware of the reporting criteria, there are often delays in transmitting the necessary information to FedCIRC. Less than full reporting makes trend analysis difficult and diminishes the ability to correlate ongoing attacks. FedCIRC is currently analyzing technical options for pulling incident data automatically from agency systems. Automating the incident reporting process would greatly increase the raw data available for analysis.

- Timely technical assistance regarding security incidents

  In January, 2003, FedCIRC launched the web enabled Patch Authentication and Dissemination Capability (PADC). PADC pushes out notices of security patches based on each agency's submitted infrastructure profile. Validated patches are then available for download from the FedCIRC website. As of September 30, 2003, 47 agencies had subscribed to PADC and there were 377 active users. Although some agencies have a high percentage of active users, other agencies are not taking advantage of this centralized service. DHS/FedCIRC is currently analyzing alternative solutions to meet agency patch management requirements.

- Consultation with NIST and NSA regarding information security incidents

  In August, 2003, FedCIRC published its incident response and report guide. This guide was developed in coordination with NIST and is meant to assist federal agencies with understanding, preparing for, responding to, and reporting IT incidents. The guide instructs agencies to protect their IT networks by maintaining current network

asset inventory profiles, conducting periodic vulnerability assessments, and updating system patches regularly.

FedCIRC uses DHS' Critical Infrastructure Warning Information Network (CWIN) to collaborate securely with agency incident response teams, DOD's Joint Task Force-Computer Network Operations, the intelligence community's National Security Incident Response Center (NSIRC) and the private sector. Additionally, it facilitates discussion on best practices, trends, and lessons learned. OMB believes that coordination between the intelligence community, civilian agencies and DOD improved in FY 2003 with information on threats and vulnerabilities being shared in a more effective manner.

Appendix B: Reporting by Small and Independent Agencies

Background

In FY 2003, OMB partnered with the Small Agency CIO Council to increase awareness of FISMA requirements. OMB and Council staff provided frequent briefings to agencies on vulnerability assessment, remediation planning and reporting. Additionally, the Small Agency CIO Council sponsored a two day training session entitled "Security for the Small Agency and Bureau Community".

Fifty-five small and independent agencies submitted FISMA reports in FY03 (a list of agencies that submitted reports is included in this appendix). Of the 55 agencies that submitted reports, 20 did not include an independent assessment that met FISMA standards. In general, the agencies cited lack of an IG and scarcity of funds as reasons for their inability to complete a comprehensive review of their agency's security program.

The small and independent agencies spent 78 million dollars for IT security in FY03. This sum does not include eight agencies that did not record the amount of money spent to protect their information and information systems.

Twenty-six agencies subject to FISMA did not submit reports in FY03. The majority of these agencies have less than 100 full time employees.

Agencies with identified Material Weaknesses

A crosscut analysis of the FISMA reports (a table of agency performance is included at the end of this appendix) shows that 23 agencies have declared at least one material weakness in management, operational or technical controls. These weaknesses include lack of security plans and policies, absence of risk management programs, inadequate contingency planning, and insufficient security awareness and training activities.

The overall number of material weaknesses at the small and independent agencies has grown from 128 in FY02 to 160 in FY03. Sixty-nine of the material weaknesses identified in FY03 were discovered in prior years. Many of the new weaknesses are due to better identification and reporting of significant deficiencies.

Identification of Mission Critical Systems

FISMA requires agencies to identify telecommunications or information systems that if subject to loss, misuse, disclosure or unauthorized access, would have a debilitating impact on the mission of an agency.

To date, 50 small and independent agencies have documented their mission critical operations and assets.

Inventory of Major IT Systems

FISMA requires the head of each agency to develop and maintain an inventory of major information systems, including an identification of the interfaces between each system and all other systems and networks. The inventory is used to support information resources management including monitoring, testing and evaluation of information security controls.

Twenty-five agencies have completed an inventory of their major information systems.

Risk Management Programs at the Small and Independent Agencies

Risk Assessment

Thirty of the small and independent agencies have assessed each of their systems for risk. The remaining agencies are divided between those that conducted risk assessments for a subset of their systems and those that conducted no risk assessments at all.

Security Plans

Twenty-six agencies have developed security plans to document the management, technical and operational controls designed to reduce risk for each of their systems. Seventeen agencies have prepared plans for a portion of their systems. Twelve agencies have no written security plans.

Certification and Accreditation

Thirteen agencies have certified and accredited all of their systems to operate within specific risk parameters. Management officials at these agencies have implemented a formal process to validate the efficacy of security controls referenced in the security plans.

The lack of certification and accreditation at the other small and independent agencies is a significant concern with 27 agencies not conducting any certification or accreditation activities.

Testing of Agency Security Controls

In accordance with FISMA, agencies must periodically test and evaluate information security controls and techniques. These tests are important in establishing areas for improvement.

Twenty-four agencies reported that they tested security controls annually for each of their systems. Thirteen agencies did not test security controls at all.

Incident Handling Programs

In accordance with FISMA requirements, agencies must institute procedures for detecting, reporting, and responding to security incidents. Civilian agencies are required to report IT security incidents to DHS' Federal Computer Incident and Reporting Capability (FedCIRC).

Although almost all small and independent agencies have policies that require incidents be reported to FedCIRC, some agencies fail to characterize abnormal system activity, such as that caused by worms and viruses, as reportable incidents. This lack of reporting decreases FedCIRC's ability to track incidents across the federal enterprise.

Two IGs were concerned about the ability of their agency to identify incidents. One wrote "The lack of monitoring tools and procedures increases the risk and likelihood that sensitive information will be improperly released and system compromise will be undetected. The (agency) would find it difficult to identify when the incident occurred and the individual involved."

Security Awareness, Training and Education

For Agency Employees Including Contractors

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

Fifteen agencies reported that they provided security training in FY03 for 100% of their staff. Fourteen trained less than 10% of their personnel.

The remaining agencies reported that their security education, training and awareness programs reached a moderate number of their workforce.

For Employees with Significant Security Responsibilities

The agencies reported that for employees with significant security responsibilities, on average 53 percent received training in FY03. Specialized instruction was provided in practices such as perimeter defense, enterprise network security, infrastructure security management and IT security capital planning.

Continuity of Operations

Plan Preparation

Although 28 agencies developed continuity of operations plans for all of their IT systems, 11 agencies had done no contingency planning. The remaining agencies had prepared plans for selected systems.

Testing

Contingency plans that are periodically tested are more viable than those that are not. Eleven 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 52% of agencies conducting any testing at all.

Remediation of Identified Security Vulnerabilities at Small and Independent Agencies

In FY03, 43 small and independent agencies submitted plans of action and milestones to OMB. 12 of these agencies are first time participants in the POA&M process.

Collectively, the agencies identified a total of 1223 weaknesses. Of this number, 664 (53%) were reported corrected by the agencies at the end of FY03.

Although the POA&M process continues to mature in terms of the number of participating agencies, the number of identified vulnerabilities, and the number of completed corrective actions, several IGs expressed concern regarding the comprehensiveness of agency POA&M processes. IG concerns included lack of management oversight, failure to adequately prioritize activities and lack of funding for remedial actions.

OMB will continue to track the completion of open POA&M items using the quarterly security updates from the agencies.

Conclusions

FISMA requires that agencies implement effective security controls in order to protect Federal information and information systems. As a group, the small and independent agencies have successfully identified their mission critical operations and assets, assessed their systems for risk and developed security plans.

Statistically, the agencies are less likely to have conducted certification and accreditation of systems or tested security controls on an annual basis. These security reviews must be done for all systems in order to protect the integrity, confidentiality and availability of agency information.

Additionally, agencies must ensure that their employees have received appropriate security training. Failure to inform employees of their responsibilities in complying with agency policies and procedures increases risk.

Finally, agencies must work diligently in the coming year to close out material weaknesses. These weaknesses, identified in FISMA as significant deficiencies in a

policy, procedure or practice must not be allowed to remain open indefinitely. OMB intends to closely monitor progress by the small and independent agencies in closing out these weaknesses.

Small and independent agencies that submitted FISMA reports:

1. Access Board
2. African Development Foundation
3. American Battle Monuments Commission
4. Appalachian Regional Commission
5. Barry Goldwater Scholarship Foundation
6. Broadcasting Board of Governors
7. Christopher Columbus Fellowship Foundation
8. Corporation for National and Community Service
9. Court Services and Offender Supervision Agency
10. Defense Nuclear Facilities Safety Board
11. Executive Office of the President, Office of Administration
12. Export/Import Bank of the United States
13. Farm Credit Administration
14. Federal Communications Commission
15. Federal Deposit Insurance Corporation
16. Federal Energy Regulatory Commission
17. Federal Housing Finance Board
18. Federal Labor Relations Authority
19. Federal Maritime Commission
20. Federal Reserve System
21. Federal Trade Commission
22. Inter-American Foundation
23. Institute of Museum and Library Services
24. Japan-US Friendship Commission
25. Marine Mammal Commission
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. Nuclear Waste Technical Review Board
35. Occupational Safety and Health Review Commission
36. Office of Federal Housing Enterprise Oversight
37. Office of Special Counsel
38. Overseas Private Investment Corporation
39. Peace Corps
40. Pension Benefit Guaranty Corporation

41. Postal Rate Commission
42. Railroad Retirement Board
43. Securities and Exchange Commission
44. Selective Service
45. Smithsonian Institution
46. Tennessee Valley Authority
47. U.S. Chemical Safety and Hazard Investigation Board
48. U.S. Commodity Futures Trading Commission
49. U.S. Consumer Product Safety Commission
50. U.S. Equal Employment Opportunity Commission
51. U.S. Holocaust Memorial Museum
52. U.S. International Trade Commission
53. U.S. Merit Systems Protection Board
54. U.S. Office of Government Ethics
55. U.S. Trade and Development Agency

Name of agency	Independent assessment provided (y/n)	Budget $ for IT security ($K)	# of material weaknesses in FY03	# of material weaknesses repeated from last year	Mission critical ops and assets identified (y/n)	% of systems assessed for risk	% of systems with security plans	percentage of systems certified and accredited	% of systems with tested security controls	Incidents reported to FedCIRC (y/n)	% of users trained	% of security staff trained	% of systems with contingency plans	% of systems with tested contingency plans	submission of FY03 POA&M?	# of weaknesses identified in FY03	# of weaknesses reported corrected as of 10/1/03
		Q. A.1	A.3	A.3	B.7	C.1	C.1	C.1	C.1	B.8	C.3	C.3	C.1	C.1			
Access B.	N	UNK	0	0	Y	100	100	0	100	N	5	100	100	0	N	0	0
ADF	N	50	UNK	UNK	Y	0	100	29	29	N	0	33	0	0	N	0	0
ABMC	N	UNK	0	0	Y	100	100	100	100	Y	UNK	UNK	100	100	N	0	0
ARC	N	15	0	0	Y	75	100	0	100	Y	100	100	100	75	N	0	0
BBG	Y	5,965	0	0	Y					Y	0	0			Y		
OCB						100	0	0	100				0	0	Y	10	9
OCS						0	0	0	0				0	0	Y	187	1
OE						100	100	0	5				10	10	Y	9	5
OIS						100	100	0	0				100	0	Y	6	4
VOA						0	0	0	0				0	0	Y	8	6
BG	N	0	0	0	UNK	0	0	0	0	N	0	0	0	0	N	0	0
CCFF	N	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	N	0	0
CNCS	Y	UNK	0	0	Y	100	100	100	100	Y	100	100	100	100	Y	4	0
CSOSA	N	1,151	0	0	Y	71	14	14	71	Y	1	6	0	0	Y	9	0
DNFSB	N	99	0	0	Y	100	12	0	0	Y	20	40	12	12	Y	17	15
EOP	VA	217	0	0	Y	100	100	100	100	Y	23	90	100	0	Y	6	5
EXIMBANK	Y	1,102	0	0	Y	100	50	0	100	Y	75	100	100	0	Y	61	25
FCA	Y	477	0	0	Y	100	100	0	100	Y	96	93	80	80	N	0	0
FCC	Y	4,100	3	3	Y	53	100	42	53	Y	100	88	5	5	Y	48	26
FDIC	Y	22,500	0	0	Y	13	100	0	25	Y	98	89	100	94	Y	10	10
FERC	Y	567	19	4	Y	91	3	3	3	Y	84	87	3	0	Y	29	11
FHFB	Y	281	4	4	Y	0	33	33	0	Y	45	NA	100	0	Y	33	25
FLRA	Y	83	0	0	Y	0	0	0	0	N	0	0	0	0	Y	46	13
FMC	Y	241	5	1	Y	100	78	65	4	Y	88	0	78	0	Y	29	14
FRB	Y	5,600	0	0	Y	100	67	93	37	Y	100	84	72	67	Y	11	1
FTC	Y	577	2	0	Y	100	100	14	0	Y	35	62	100	100	Y	16	14
IAF	N	77	18	0	Y	100	100	0	100	Y	26	44	100	0	Y	18	5
IMLS	N	30	0	0	Y	100	0	0	0	Y	82	50	0	0	Y	7	1
JUSFC	N	3	0	0	Y	100	100	0	100	Y	100	100	100	100	N	0	0
MKUDALL	N	2	0	0	N	0	0	0	0	N	0	0	0	0	N	0	0
MMC	N	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	N	0	0
NARA	Y	2,400	2	2	Y	100	100	100	100	Y	62	100	100	0	Y	12	6

Name of agency	Independent assessment provided (y/n)	Budget $ for IT security ($K)	# of material weaknesses in FY03	# of material weaknesses repeated from last year	Mission critical ops and assets identified (y/n)	% of systems assessed for risk	% of systems with security plans	percentage of systems certified and accredited	% of systems with tested security controls	Incidents reported to FedCIRC (y/n)	% of users trained	% of security staff trained	% of systems with contingency plans	% of systems with tested contingency plans	submission of FY03 POA&M?	# of weaknesses identified in FY03	# of weaknesses reported corrected as of 10/1/03
NCUA	Y	946	2	1	Y	85	85	62	85	Y	24	61	92	8	Y	168	154
NEA	Y	17	0	0	Y	100	100	100	100	Y	21	18	100	100	Y	4	3
NEH	Y	50	2	0	Y	100	100	100	100	Y	100	100	100	100	Y	3	1
NGA	N	90	8	8	Y	17	17	0	0	Y	0	5	17	8	Y	10	2
NLRB	Y	473	3	2	Y	40	100	100	60	Y	55	100	60	0	Y	158	140
NMB	N	0	0	0	Y	100	100	100	100	Y	100	100	100	100	Y	2	1
NWTSB	N	UNK	9	5	Y	100	0	0	0	N	94	33	100	0	Y	9	4
OFHEO	Y	170	0	0	Y	0	0	0	100	Y	99	15	100	100	Y	4	0
OPIC	Y	231	7	0	Y	100	0	0	100	N	1	50	100	0	Y	25	21
OSC	N	UNK	0	0	Y	100	100	0	100	Y	100	100	100	100	Y	1	0
OSHRC	Y	87	2	2	Y	100	100	0	100	Y	96	100	100	0	Y	11	8
PBGC	Y	3,550	4	4	Y	50	100	50	20	Y	100	100	100	60	Y	18	5
PCORPS	Y	2,200	31	16	Y	46	25	25	54	Y	95	100	85	70	Y	18	4
PRC	VA	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	UNK	N	0	0
RRB	Y	2,023	1	1	Y	100	100	100	22	Y	100	44	100	66	Y	10	5
SEC	Y	13,271	1	1	Y	0	2	0	2	Y	4	25	2	57	Y	39	21
SMITHSO	Y	1,193	0	0	Y	92	92	0	17	Y	62	11	8	8	Y	22	14
SSS	Y	127	0	0	Y	100	100	100	100	Y	100	0	100	50	Y	2	1
TVA	Y	3,200	5	4	Y	27	27	18	50	Y	94	20	23	23	Y	8	2
USCFTC	Y	309	0	0	Y	100	71	0	14	Y	87	100	71	0	Y	29	10
USCPSC	Y	715	0	0	Y	100	100	100	100	Y	0	56	100	100	Y	8	8
USCSHIB	Y	8	3	2	Y	0	0	0	100	Y	100	100	100	100	Y	16	7
USEEOC	Y	1,297	0	0	Y	100	100	100	100	Y	100	100	100	71	Y	20	20
USHMM	Y	183	2	2	Y	100	50	8	66	Y	1	33	66	66	Y	20	17
USITC	Y	430	0	0	Y	29	57	14	0	Y	86	29	0	0	Y	15	7
USMSPB	Y	182	15	7	Y	100	100	100	100	Y	100	33	0	0	Y	15	13
USOGE	Y	346	12	0	Y	100	100	0	100	Y	100	100	0	0	Y	12	0
USTDA	N	69	0	0	Y	100	0	0	100	Y	0	0	100	0	N	0	0

Appendix C: Individual Agency Summaries for the 24 CFO Agencies

This appendix provides summaries of agency and IG FY 2003 FISMA reports. Please note that these summaries only cover activities undertaken in FY 2003.

Agency for International Development

IT Security Background

USAID reported one program, eight systems, and three contractor operations and facilities. USAID review of its program, three systems and one contractor facility used NIST guidelines. The agency reported two material weaknesses, of which both were repeated from last year. These weaknesses were included in the agency's POA&M process. All eight systems integrated security control costs into the life cycle of the system. Three incidents were identified and reported to FedCIRC.

Management and Program Performance Highlights Reported by Agency

- USAID issues system vulnerability grades to each system owner and system manager, as well as to the chief information security officer. Grades are based on the number and severity of vulnerabilities found during monthly scanning and vulnerability reviews.
- All new employees, including contractors, receive security awareness training prior to issue of agency badge.

Management and Program Performance Highlights Reported by the OIG

- USAID has an effective POA&M process.

Management and Program Performance Challenges Reported by Agency

- While new personnel receive training, USAID has not yet tracked the security training provided to existing personnel.

Management and Program Performance Challenges Reported by the OIG

- USAID does not have a complete system inventory, and some systems have yet to be incorporated in agency FISMA reviews.
- Work remains to ensure sensitive data is not exposed to unacceptable risks of loss or destruction.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Agency for International Development FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**8**	**8**	100%	**7**	88%	**7**	88%	**8**	100%	**1**	13%	**1**	13%	**0**	0%

The agency reports the CIO maintains an agency-wide IT security program and evaluates IT security performance of agency bureaus. Monthly vulnerability scans, supported by the agency chief information officer, help ensure the CIO that components are complying with IT security policies. The agency is working to include all weaknesses into the POA&Ms. The OIG reported weaknesses in the agency's training program, and roughly half of all agency employees received security awareness training. The agency reports all new employees have received IT security training, and over three-fourths of agency employees with significant IT security responsibilities received specialized security training.

Responsibilities of Agency Head

The agency reports the agency head designated the agency's Chief Information Security Officer (CISO) as responsible for IT security responsibilities as detailed in FISMA. The CISO is supported by associate information security officers in oversees missions. Additionally, the agency head authorized and reviews monthly vulnerability assessments, and prevents operating components from making major IT investments without the concurrence of the CIO. While the agency head is working to integrate security into the capital planning process, the OIG reported the policy for developing security documents throughout the systems life cycle does not appear to be documented. The agency reported that the agency head directed the CIO to issue scores to all agency components for their progress in IT security implementation to provide feedback to system owners and managers on their compliance to agency security policy. PDD 63 assigns the Department of State responsibility for coordinating the critical infrastructure protection efforts for foreign affairs agencies and as of yet, the agency reports the Department of State has not assigned CIP responsibilities to USAID. Separate staffs at USAID are devoted to other security programs, including the physical security of agency resources, to avoid duplication of efforts. There are no national critical operations and assets at USAID, and all mission critical operations and assets – as well as their interdependencies and interrelationships – have been fully identified. The agency reports that the agency information security officer is responsible for reporting incidents to FedCIRC, and confirmation of patch installation occurs during monthly vulnerability scanning. The

agency develops configuration requirements including patching of security vulnerabilities.

U.S. Department of Agriculture

IT Security Background

USDA reported 204 programs, 271 systems, and 22 contractor operations and facilities at 23 bureaus. This year's FISMA review included 116 programs, 193 systems, and 17 contractors operations, and the Department used NIST's self-assessment guide. The Department has not yet completed an inventory of major IT systems and not all material weaknesses are included in their POA&M process. One hundred incidents were reported, fifty-four were reported externally to FedCIRC. Ninety-two percent (249 of 271) of all systems integrated security control costs into system life cycle management. OIG reports ninety-four material weaknesses, of which twenty were repeated from last year, in key areas including access controls, identification and mitigation of vulnerabilities, and management commitment in the Department's IT security program.

Management and Program Performance Highlights Reported by the Department

- The Secretary of Agriculture established an information security performance measure as part of consideration during each Department executive's annual performance review.
- The Department revised the Capital Planning and Investment Control Guide to ensure new investments adequately incorporate security requirements throughout the investment life cycle.

Management and Program Performance Highlights Reported by the OIG

- The OCIO has an effective incident response program which includes an intrusion detection process to communicate known vulnerabilities and identify patches as well as a direct line of communication to FedCIRC, although not all Department officials, components, and bureaus are integrated into the response program.

Management and Program Performance Challenges Reported by the Department

- 80% of Department operational systems have not been certified and accredited.
- The Department has not begun identification of mission and national critical operations and assets.

Management and Program Performance Challenges Reported by the OIG

- A number of weaknesses exist in the Department's POA&M process, including lack of POA&Ms for all systems and programs, incomplete accounting of all weaknesses, and limited integration of resources needed for corrective action.

Responsibility of Agency Program Officials and CIO

Table C.1 of the U.S. Department of Agriculture FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**271**	**196**	85%	**182**	86%	**37**	20%	**249**	92%	**83**	47%	**155**	62%	**79**	39%

The Department reports the OCIO has established a process to verify compliance with the Department security policy, but not all bureaus are yet involved in the process. A Department information security officer works in the OCIO to implement Department security policy. The OIG reported the OCIO maintains a shared database, but POA&Ms do not contain weaknesses at all Department bureaus. The Department reports roughly half of all Department employees received IT security awareness training and 78% of employees with significant security responsibilities received specialized IT security training.

Responsibilities of Agency Head

The Department reported the Department head promulgated Department security policies and procedures which identify responsibilities and authorities to comply with FISMA and the Department's IT security program. Additionally, all IT acquisitions greater than $25,000 are approved by the CIO, and OCIO reviews each acquisition to ensure appropriate IT security considerations are part of the process. While the Department uses on-site and independent reviews, as well as self-assessments and other reviews to oversee compliance with Department security policy, the OIG reported that Department security plans are not always practiced throughout the life cycle of the system. A Homeland Security Administrative Infrastructure Working Group facilitates the integration of the Department's security program with critical infrastructure responsibilities and other security programs. Not all Department mission and national critical assets and operations have been identified, and the Department will be partnering with DHS to conduct a review to identify those assets and operations. The Department reports specific configuration requirements, including requirements to address patching, have been developed.

Department of Commerce

IT Security Background

DOC reported 14 bureaus implementing 34 programs supported by 552 systems and 37 contractor operations and facilities. All of the programs and 550 systems were reviewed as part of the FISMA report. While the Department is still validating their systems inventory data, pertinent security information on all DOC systems, including information on each system's compliance with IT security requirements, system contacts, and system description is maintained in the inventory and used to assess compliance with the security program. The OIG recommended the Department continue to report information security as a material weakness until all national and mission critical systems have been certified and accredited. The OIG evaluation found numerous Department systems reported as certified and accredited have significant deficiencies in their certification and accreditation materials. Over 73,000 incidents were reported, of which 70,985 were reported to FedCIRC. Eighty-nine percent of all operational systems integrated IT security costs into the system life cycle.

Management and Program Performance Highlights Reported by the Department

- A new information security policy delineates CIO and program official roles and responsibilities. The CIO has primary oversight of the Department's information security program and reports directly to the Deputy Secretary while program officials ensure implementation for the IT security program for systems under their responsibility.
- The OCIO has initiated a compliance review program to evaluate the performance of all department operating units by validating the security information they report and assessing the effectiveness of their information security programs.

Management and Program Performance Highlights Reported by the OIG

- DOC manages an effective POA&M process and is working to better tie weaknesses to budget requests.

Management and Program Performance Challenges Reported by the Department

- Bureaus at the Department vary significantly in the numbers of reported incidents.

Management and Program Performance Challenges Reported by the OIG

- The quality of DOC's risk assessments, security plans, security control testing, and certification and accreditation lacked essential information, and were often inconsistent or inaccurate.
- Complete identification of national and mission critical operation and asset interdependencies and interrelationships must continue.

Responsibilities of Program Officials and CIO

Table C.1 of the Department of Commerce FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**555**	**555**	100%	**555**	100%	**541**	97%	**495**	89%	**502**	90%	**549**	99%	**421**	76%

The Department reports the CIO has primary oversight of all aspects of Commerce's information security program and reports to the Deputy Secretary on the status of information security within the Department. Operating unit heads and program officials are responsible for implementing an effective information security program for systems under their responsibility. Furthermore, the CIO has designated a senior information security officer and a Commerce Critical Infrastructure Program Manager ensures the stability of operational and technical security controls within the Commerce IT infrastructure and manages the Department's Computer Incident Response Team (CIRT). The Department reports 94% of DOC's 48,269 employees and contractor employees received security awareness training in the last year. While 100% of employees with significant security responsibility have received specialized training, the OIG reports inconsistent training requirements for these personnel and the need for an improved understanding of their duties and responsibilities.

Responsibilities of Agency Head

The Department reports the Secretary of Commerce oversees all IT security activities within the Department. The roles and responsibilities for IT security are defined in the Department's IT Security Program Policy issued in January 2003. Additionally, the Secretary of Commerce formally delegated FISMA responsibilities to the Department CIO, who in turn has formally designated a senior program manager to oversee implementation of and compliance with FISMA requirements within the Department. Operating units can not make a major IT investment decision without concurrence of the CIO. Other security programs such as operations planning, personnel security, and physical security, is under the authority of the Department's Chief Financial Officer who coordinates security efforts with the CIO to avoid duplication. DOC reports the Department head ensures the Department's information security plan is practiced throughout the lifecycle of each agency system by directing employees to support the department's 5-stage security lifecycle process. While the Department has identified mission and national critical operations and assets, work remains to fully identify their interdependencies and interrelationships. The Department reports a formal process is in place for timely dissemination of vulnerability information and patching solutions, and configuration requirements – including patching – have been developed.

Department of Defense

IT Security Background

DoD reported 1,475 unclassified circuits, 3,557 systems, and 4,716 contractor facilities. 1,458 circuits, 378 systems, and 4,000 contractor facilities were reviewed as a basis for this report. The Director of Defense Security Service is responsible for ensuring contractor facilities are adequately secure. In lieu of the NIST self-assessment guide, DoD uses the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) to conduct their reviews. The Department confirms the DITSCAP process covers the necessary elements of the NIST guidelines. The six material weaknesses reported were repeated from last year and are integrated into Department POA&Ms. All 42,421 IT security incidents identified in FY03 were reported directly to FedCIRC. Sixty-seven percent of sampled systems integrated security costs into the system life-cycle.

Please note that the FY03 DOD IG report had not yet been submitted at the time the OMB report was issued. Therefore, there is no reference to IG findings in this summary.

Management and Program Performance Highlights Reported by the Department

- The Department promulgated an Information Assurance Strategy that serves as a planning and management guide for all Services and Agencies and helps ensure a consistent approach to assuring information across DoD.
- The Department uses a consistent process to review the security controls of operational systems.
- DoD is improving its system certification and accreditation practices and associated databases to better track systems in the certification and accreditation process.

Management and Program Performance Challenges Reported by the Department

- DOD has not fully identified the interrelationships and interdependencies of its national and mission critical operations and assets.
- The Department provided a sample set of its major information systems to complete the FISMA report, and as a result, its IT security findings represent a sample of DoD's total IT portfolio. Plans are in place to report on all systems for the FY 2004 reporting cycle.
- Implementation of the Information Assurance Vulnerability Alert process to facilitate compliance and implementation of patches is not complete at all agencies and Services.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Defense FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**378**	**343**	91%	**334**	88%	**302**	80%	**242**	64%	**157**	42%	**299**	79%	**191**	51%

The Department reports that the CIO chairs an Executive Board comprised of all Department CIOs to focus on information security goals. The Deputy CIO chairs an Information Assurance Senior Group to develop and enforce IT security policy and implementation. Additionally, the CIO reviews the IT security performance of all components through development of the FISMA report as well as the Annual Information Assurance Report to Congress. The CIO has appointed a chief information security officer who monitors and evaluates IT security activities. The Department reports eighty-four percent (2,463,748) of all employees received IT security awareness training, and ninety percent (40,364) of employees with significant IT security responsibility received specialized IT security training.

Responsibilities of Agency Head

The Department head endorses the Information Assurance Strategy to articulate security program objectives and guidelines. The DoD CIO reviews IT investment decisions and provides advice to the Secretary of Defense on all IT investments. To oversee the IT security performance of agency program officials, the Assistant Secretary of Defense for Networks and Information Integration presents quarterly updates to the CIO Executive Board on certification and accreditation progress and other potential IT security issues to best allocate IT security corrective actions and resources. The Department reports that critical infrastructure protection responsibilities are integrated with IT security and other security programs. Separate staffs and agency officials are devoted to other security programs so as to avoid duplication and ensure consistency. The Department is using a tool to assess all assets and determine how to best mitigate the risk and impact of their potential loss. The Department reports they have developed configuration requirements, including requirements for patching of vulnerabilities.

Department of Education

IT Security Background

Education reported 23 programs, 76 systems, and 13 contractor operations and facilities across 23 Principal Offices at the Department. The NIST self-assessment guide was used to review all programs, systems, and contractor operations and facilities. In FY03, the Department's OIG identified 66 material weaknesses for each of the Department's systems operating without a completed certification and accreditation, and an additional material weakness for the Department's overall IT Security Program. As a result, the OIG finds the Department is still not in full compliance with FISMA although improvements have been made. The Department identified 10 incidents defined as successful intrusions into the Department's network, and all were reported externally to FedCIRC. Fourteen percent of the Department's systems integrated security costs into system life cycle.

Management and Program Performance Highlights Reported by the Department

- Key information security policies and procedures have been finalized, documented, and disseminated to support the Department's information security program.
- The Department has identified mission critical operations and assets.

Management and Program Performance Highlights Reported by the OIG

- The Department has a robust POA&M process that effectively manages and prioritizes security weaknesses, although system level POA&Ms can be tied more fully to system budget requests.

Management and Program Performance Challenges Reported by the Department

- At the end of FY03, ten of seventy-six operational systems had obtained certification and accreditation. The Department plans to complete C&A for all mission critical systems in FY04 and the remaining systems in the first quarter of FY05.

Management and Program Performance Challenges Reported by the OIG

- Incident handling and response capability is inconsistent across the Department, particularly in operating environments involving contractors.
- Department servers were operating with known vulnerabilities, which allowed unauthorized access to Department information and records. This was caused primarily by a lack of timely distribution of patches and effective testing and verification of patch application and corrective actions.

Responsibilities of the Agency Program Officials and CIO

Table C.1 of the Department of Education FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**76**	**76**	100%	**69**	90%	**10**	13%	**11**	14%	**75**	99%	**36**	47%	**68**	89%

The Department reports the CIO provides program officials with instructions on how to comply with IT security mandates, and the OCIO evaluates the performance of Principal Offices. The OCIO also plans to use results from the certification and accreditation process to validate these office's compliance with FISMA, and will include uncovered weaknesses in the Department's POA&M process. The OIG reports the Department had not formally identified a senior information security officer. The Department reported seven percent of Department personnel received security awareness training, although employees were required to complete security awareness training a month after completion of the Department's FISMA report. All employees with significant security responsibilities received specialized training.

Responsibilities of the Agency Head

The Department reports that their IT Security Program Management Plan (ITSPMP) outlines the Department head's IT security responsibilities and delegates security responsibilities to the CIO and program officials. The ITSPMP also describes how the Department head will oversee annual reviews, audits and certification and accreditation programs. The Department head has approved an IT Security System Development Lifecycle Guide to help integrate information security policies into system life cycle development. The CIO leads an investment review board to prevent major operating components from making an IT investment decision without CIO concurrence. Separate staffs coordinate to avoid duplication of personnel, physical, and information security efforts. The Department has no national critical operations and assets and has identified all mission critical operations and assets. Twelve Principal Offices have incident handling and response capability, but the OCIO has sole responsibility for reporting to FedCIRC. Specific configuration requirements, including the patching of known vulnerabilities, are developed and complied with for the Department.

Department of Energy

IT Security Background

DOE reported eight programs, 1,172 systems, and 32 contractor operations/facilities. All programs and contractor operations and facilities, and 89% of all agency systems were reviewed as part of this report. Ninety-seven percent of all self-assessments did not use the NIST self-assessment guide, but explicit guidance was issued in May 2003 directing all components to exclusively use the NIST self-assessment guide. DOE reported 1,926 security incidents of which 89 were reported to FedCIRC. Neither Agency officials nor the Inspector General identified any material weaknesses for the Department's IT security systems. DOE reported 95% of all operating systems integrated security costs into the system life cycle.

Management and Program Performance Highlights Reported by the Department

- The Department of Energy led a team consisting of some agency and industry experts which developed a security benchmark for Oracle Databases. The benchmark has been adopted by DOE, other agencies and the Center for Internet Security. DOE negotiated an enterprise license agreement with Oracle under which Oracle pre-configures the Oracle database to the benchmark. The agreement also includes configuration and pre-testing of any subsequent security patches.
- Agency quarterly reporting to the OCIO on key IT security measures better identifies where security policies and implementation are incomplete or inconsistent. This improves the Department's ability to focus attention on areas of greatest need.
- Perimeter sensors are installed at 18 large DOE sites and headquarters to identify, track and report potentially malicious activity such as scans, probes, and unsuccessful log-on attempts.

Management and Program Performance Highlight Reported by the OIG

- DOE manages an effective POA&M process and will work to more consistently tie POA&M weaknesses to the agency budget and have agency program officials report to the CIO on a more regular basis.

Management and Program Performance Challenges Reported by the Department

- DOE reported 68% of all systems have contingency plans and 27% of those plans have been tested. This could cause loss of support to critical and sensitive operations.
- Due to continued under use of NIST self-assessment guidance, explicit requirements to use NIST guidance was issued in May 2003.

Management and Program Performance Challenges Reported by the OIG

- Agency programs and sites have broad discretion in determining what incidents are reported and half of the Department's organizations did not report incidents.

Responsibilities of Agency Program Officials and CIO

Table C.1 of the Department of Energy FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**1172**	**1041**	89%	**1075**	92%	**970**	83%	**1112**	95%	**1014**	87%	**792**	68%	**316**	27%

The Department reported the CIO is responsible for overseeing an agency-wide IT security program and for evaluating the performance of IT security programs thru OIG and GAO reviews, assessments conducted by the Office of Independent Oversight and Performance Assessment, peer reviews, and other independent assessments. These reviews provide a basis for the quarterly cyber-security scorecard which is tied to the agency POA&M. Additionally, quarterly security scorecards and POA&Ms help the CIO ensure that program offices are complying with DOE's security program guidelines. Agency IT security awareness training reached 92% of agency employees and 95% of employees with significant security responsibilities received specialized security training in diverse topics including: Computer Forensics, Computer Sanitization, and IT Counterintelligence Training.

Responsibilities of the Agency Head

The Department reports the agency head formally assigned IT security responsibility to the OCIO and an overall agency cyber security management program was established. The agency head ensures that the agency's information security plan is practiced throughout the lifecycle of each agency system by preventing operating components from making major IT investments without approval of the OCIO and delegating the OCIO to review capital asset acquisition plans to ensure security costs are adequately integrated into system expenditures. The Department reported the agency head established a DOE Management Challenges initiative to identify and track corrective actions which are to be reported monthly by the CIO to the agency head. An Integrated Security and Safeguards Management Program drives coordination between the IT security program and critical infrastructure responsibilities and physical security operations. Separate staffs are responsible for physical, personnel and information security, as well as continuity of operations efforts. The OIG reports DOE has fully identified national critical operations and assets, but has not yet fully identified the interdependencies and interrelationships between them. Furthermore, mission critical operations and assets have not been identified. The OIG reported all department program offices and their field elements are to report incidents to their on-site cyber security official who then report to DOE's Computer Incident Advisory Capability (CIAC). The CIAC is the sole component responsible for reporting to FedCIRC.

Environmental Protection Agency

IT Security Background

EPA reported 24 programs, 164 systems and 77 contractor operations and facilities. All programs and systems and 48 contractor operational and facilities were reviewed. Reviews adhered to NIST risk-assessment methodology, and included physical inspections and system penetration testing. The Agency IT security program did not report any material weaknesses. Eighty-six percent (141 of 164) of operational systems integrate security control costs into the system life cycle. The Agency developed the ASSERT system to maintain its system inventory. EPA reported 2,700,171 incidents, of which all were reported to FedCIRC.

Management and Program Performance Highlights Reported by the Agency

- EPA uses an automated tool for managers to gather system data in support of the annual FISMA report and IT security reviews. Results from the reports are basis for internal scorecards of agency executives to measure their IT security performance.
- Almost all (94%) systems operate with a complete certification and accreditation.

Management and Program Performance Highlights Reported by the OIG

- EPA manages an effective POA&M process, and is working to prioritize security weaknesses more appropriately.

Management and Program Performance Challenges Reported by the Agency

- A majority (69%) of employees with significant security responsibilities did not receive specialized training, although almost all employees received IT security awareness training.
- Roughly 40% (29 of 77) of agency contractor operations and assets were not reviewed as part of this report.
- While a majority of systems have contingency plans, 70% of all operational systems have not yet had those contingency plans tested.

Responsibility of the CIO and Agency Program Officials

Table C.1 of the Environmental Protection Agency FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested**	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**164**	**164**	100%	**154**	94%	**154**	94%	**141**	86%	**144**	88%	**132**	80%	**49**	30%

The agency reported the CIO maintains an agency IT security program managed by the security staff under the Deputy CIO for Technology, who is responsible for overseeing development, maintenance and implementation of the Agency-wide security program, and has direct oversight and testing authority for all Agency IT operations. The CIO ensures all segments of the agency comply with the agency-wide IT security program by requiring each program office to submit IT security data that can be used to track progress on corrective actions. Additionally, the CIO also tracks annual security self assessments and conducts penetration tests to evaluate agency IT security performance. The OCIO reports 96% of agency employees received IT security awareness training.

Responsibilities of the Agency Head

The agency reports the agency head delegated specific and general IT security responsibilities under FISMA to the CIO. The agency head sponsors the Quality Information Council, chaired by the CIO, which facilitates regular communication with senior agency officials on IT security matters. Major operating components cannot make IT investment decisions without review by and concurrence of the Agency CIO. The OIG reports the CIO ensures the Agency IT security plan is practiced throughout the life cycle of each system by reviewing selected security plans and developing POA&Ms when weaknesses were present. The agency reports the agency head conducts assessments on a sub-set of investments to validate the implementation and effectiveness of the IT security controls. EPA's information technology security program, continuity of operations program, and physical and operational security programs are managed by separate offices, and the OIG reports EPA has taken steps to integrate its critical infrastructure protection responsibilities with other security programs. Separate staffs are devoted to other security programs so as to prevent duplication or inconsistency. The OIG reports EPA completed a preliminary identification of its national critical operations and assets, but has not fully identified their interdependencies and interrelationships. Additionally, mission critical operations and assets and their interdependencies and interrelationships have been identified. The Computer Security Incident Response Capability (CSIRC) team is responsible for communicating directly with FedCIRC, and is also responsible for vulnerability patch notification and tracking. Configuration requirements are developed to include patching of IT security vulnerabilities.

General Services Administration

IT Security Background

GSA reported one program, 75 systems, and 36 contractor operations and facilities. The IT security program used the NIST self-assessment guide to review GSA's program, all systems, and 20 contractor operations and assets as basis of this report. The agency reported zero material weaknesses. The agency reports that eighty-four percent (56 of 67) of all operational systems integrated IT security costs into the system life-cycle, and off 48,169 incidents reported by the agency, 99% were reported externally to FedCIRC.

Management and Program Performance Highlights Reported by the Agency

- GSA developed a vulnerability mitigation program to scan and examine the effectiveness of in-place system security controls and measure compliance with GSA objectives and policies.
- The agency has designated a Senior Agency Information Security Officer who leads a newly established Security Division. The Security Division serves under the CIO and is responsible for management, implementation, and oversight of the IT security program.
- The agency head and senior executives review agency POA&Ms and IT security measures on a quarterly basis.

Management and Program Performance Challenges Reported by the Agency

- Seventy-eight percent of agency systems have not been fully certified and accredited.

Management and Program Performance Challenges Reported by the OIG

- Weaknesses in the agency POA&M process included the omission of some security weaknesses, inadequate linkage of weaknesses to system budget requests, and inappropriate prioritization of weaknesses.
- Not all employees with significant IT security responsibilities completed specialized security training.

Responsibilities of the Agency Program Officials and CIO

Table C.1 of the General Services Administration FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**67**	**37**	55%	**37**	55%	**15**	22%	**56**	84%	**39**	58%	**30**	45%	**21**	31%

The agency reports over half of agency systems have completed risk-assessments and IT security plans, but the percentage of systems with completed certifications and accreditations remains low. The agency reports that the agency CIO, supported by a Senior Agency Information Security Official, serves as the focal point for the Agency's IT security program and is responsible for implementing agency security requirements and policies. Additionally, the OCIO works to incorporate security considerations throughout the life cycle of systems, and conformance to agency IT security policies and procedures is reviewed during certification and accreditation reviews, development of the FISMA report, and quarterly POA&M reviews. The agency reported almost all (97%) agency employees received IT security awareness training. The OIG reported half of information system security officers received specialized security training, but the total percentage of all employees with significant security responsibilities who had received specialized training was unknown.

Responsibilities of the Agency Head

The agency reports the agency head sets forth the IT security responsibilities and jurisdiction of the CIO and program officials by distributing agency IT security policies and guidelines. The guidelines outline the roles and responsibilities of all agency officials with significant security responsibilities. The agency reports the Senior Agency Security Official serves as a central security management focal point and directs the Security Division in the OCIO to manage the agency's IT security program. Additionally, all major IT investments must follow the agency capital planning and investment control process, including senior level review and concurrence. The OIG reports that the agency head is briefed quarterly on GSA's POA&M status to help ensure GSA's IT security program is implemented. The agency reports GSA has integrated the IT security program with its critical infrastructure protection capabilities and other security programs so as to minimize duplication of effort and assure consistency. The OIG reports GSA has fully identified national critical operations and assets, but not all of their interdependencies and interrelationships. Additionally, mission critical operations and assets have not been fully identified. The agency reports that agency components communicate incident information to the OCIO Security Division, which reports directly

to FedCIRC. The agency reports it has developed and complies with specific configuration requirements, including patching of known vulnerabilities.

Department of Health and Human Services

IT Security Background

HHS reported 222 systems, 13 programs, and 77 contractor operations and facilities. Eleven (or 85%) programs, 179 (or 81%) Department systems and 66 (or 86%) contractor operations were reviewed for this report. One material weakness was reported, in the Centers for Medicare and Medicaid Services (CMS) operational division. This material weakness is an accumulation of findings at the Medicare fee-for-service contractor operations, as well as the CMS Central Office. Principal vulnerabilities were in the areas of access controls, systems software, and entity-wide security planning. The Department states that there has not been any evidence that this weakness was exploited, and that CMS has requested, received, and reviewed corrective action plans for each of the vulnerabilities categorized under the material weakness. HHS reported 348,998,595 security incidents of which 13 were reported to FedCIRC. Eighty-seven percent of all operational systems integrated security control costs into system life cycle.

Management and Program Performance Highlights Reported by the OIG

- HHS has made strides in establishing a Department-wide system security program. Once the project is completed, the Department will be able to improve it's overall IT security posture, ensure enterprise-wide security standards, support integration of IT security into lines of business, and promote an environment where employee actions reflect the importance of IT security.
- HHS has implemented a Department-wide intrusion detection system, and scans Department and operational division networks.
- HHS has allocated supplemental funding to access control, claims processing system security plan development, and other high priority safeguards.

Management and Program Performance Challenges Reported by the OIG

- HHS's distributed network environment continues to present a challenge for the Department to establish a control environment that protects critical assets and creates an enterprise-wide baseline of core security requirements.
- Operating Divisions did not always conduct the required security-related system development life cycle activities, and maintain the required supporting documentation. Deficiencies were noted in the areas of risk-assessments, system security plans, contingency plans, certification and accreditation, and annual self-assessments.
- The POA&M tracking process did not include all new findings and identified weaknesses, and, findings remained open for extended periods at several operational divisions. Also, of 71 total identified deficiencies, 26 were unresolved from the prior year.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Health and Human Services FY2003 FISMA Report															
	Total Number of Systems	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**222**	**153**	69%	**177**	80%	**90**	41%	**194**	87%	**138**	62%	**107**	48%	**60**	27%

The Department describes their IT Security Program to include security policy, planning, initiatives, and projects as a single, integrated effort based on cooperation between the Department's CIO and its Operational Divisions (OPDIV). Within this effort, security of HHS networks is handled in a coordinated fashion, with implementation primarily an OPDIV responsibility. Each OPDIV has a single, integrated IT security program operationally focused on its customers and line of business. The Department states that the CIO promulgates IT security standard expectations to all OPDIV program officials throughout the year, and offers assistance in the development of processes to enhance compliance with federal and departmental requirements.

Responsibilities of Agency Head

As stated in the Department report, the Secretary has authorized the CIO to establish the Office of Security Development, Implementation, and Oversight. As authorized, the Director of this office is charged with upholding the functional responsibilities of the Chief Security Officer to maintain an enterprise-wide IT security program integrated with the strategic and operational planning process. As part of the capital planning process, the Departmental components can not make IT investment decisions without a review and concurrence by the Departmental CIO. The Department states that they ensure federal mandates, such as IT security standards, policies, training and review, are included in the capital planning process.

Department of Homeland Security

IT Security Background

DHS reported 56 programs, 347 systems, and 41 contractor operations and facilities at eleven bureaus. Using the NIST self-assessment guide, DHS reviewed fifteen programs, 152 systems and twenty-nine contractor facilities. The Department reported ten material weaknesses, and all have been incorporated into the Department's POA&M process. One-hundred and ninety-three security incidents were reported and twelve of them were reported to FedCIRC. Twenty-two percent of all operational systems integrated security costs into the system life cycle.

Management and Program Performance Highlights Reported by the Department

- Department IT security policies and procedures have been developed and disseminated, and are web accessible for Department employees.
- An Information Security Organization, headed by the Department's chief information security officer, and the Information Systems Security Board was established to provide Department IT security guidance and promulgate best practices and key security considerations throughout the Department's various components and bureaus.
- An IT Capital Planning and Investment Control and Portfolio Management Directive have been developed to better address security costs and considerations throughout the IT investment process.

Management and Program Performance Challenges Reported by the Department

- Eight percent of Department employees have received information security training and lack general awareness of the Department's IT security policies and expectations.
- The Department has not identified mission and national critical operations and assets, but a working group led by the chief information security officer will begin the asset identification process in the first quarter of FY 2004.

Management and Program Performance Challenges Reported by the OIG

- While the Department acquired an enterprise-wide POA&M management tool, the OIG does not verify a thorough POA&M process exists at the Department due to not having all systems and program weaknesses included in the POA&M, irregular reporting to the CIO of the POA&M status, insufficient linkage of POA&M weaknesses to budget requests, and lack of prioritization of system weaknesses.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Homeland Security FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**346**	**147**	43%	**155**	45%	**145**	42%	**152**	44%	**65**	19%	**123**	36%	**44**	13%

The above numbers reflect the results of the OCIO review and while generally consistent with the OIG's findings, the OIG reported fewer systems having completed each activity above except for the number of systems for which security controls were tested and evaluated. The Department reported the chief information security officer, working with the CIO, oversees implementation of Department security policy in accordance with DHS's Information Security Strategic Plan. The CIO was unable to review the IT security performance of all Department bureaus, but one key goal of the program is to fully consolidate information security programs from across the different bureaus to ensure consistency in Department policies and procedures. The Department is working to integrate information security training capabilities that exist in various bureaus. Of the Department's 208,785 employees, 8% have received IT security awareness training, and 47% of employees with significant IT security responsibility have received specialized training. The OIG reports an IT Security Training and Awareness Working Group has been established and a web-based security awareness training course is under development to better address training priorities.

Responsibilities of Agency Head

DHS reports the Department head delegated information security responsibilities to the CIO who implements a Department security plan in coordination with the agency chief information security officer. Major IT investment decisions are not made without the review of the CIO, who verifies appropriate IT security considerations are included in IT investment decisions. Physical and personnel security responsibilities fall under the DHS Office of Security, and the chief information security officer works collaboratively to prevent duplication and ensure consistency in Department security policies. The Department reports sharing incident information with FedCIRC immediately upon detection. The Department has not been able to confirm patches have been tested and installed in a timely manner, and is preparing explicit guidance to prevent patch management shortcomings. The Department reports having developed and complied with configuration requirements, including patching of security vulnerabilities.

Department of Housing and Urban Development

IT Security Background

HUD reported 9 programs, 197 systems, and 2 contractor operations and facilities. All programs, Department systems, and contractor operations or facilities were reviewed for this report. Three material weaknesses were reported by the OIG. HUD reported 1 security incident in this report, and this incident was also reported to FedCIRC. The Department also reported that 100% of all operational systems integrated security control costs into the lifecycle of the systems.

Management and Program Performance Highlights Reported by the Department

- The Department reports that they have established a Computer Incident Response Team, including network engineers and incident analysts who monitor and report on all network operations in both the intranet and internet environments.
- HUD engages in annual independent penetration testing for both internal and external HUD network resources, and performs self-initiated testing and assessments of network resources to mitigate exposure to risk and vulnerabilities.
- HUD has established a security domain as part of their Department's Enterprise Architecture. The domain sets forth the governing principles for security objectives of confidentiality, integrity, and availability. In addition, the security domain addresses security services and technologies used to sustain consistent security policy and rules across the enterprise.

Management and Program Performance Challenges Reported by the Department

- The POA&M is not being used as the authoritative management tool to identify and monitor agency actions for correcting information and IT security weaknesses.
- At the time of the report, the Department had certified and accredited 9% of their systems.

Management and Program Performance Challenges Reported by the OIG

- HUD has not followed NIST guidelines for the development and testing of contingency related plans, resulting in inadequate assurance that HUD can recover computer processing operations in the event of a disaster or other unexpected interruption.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Housing and Urban Development FY2003 FISMA Report															
	Total Number of Systems	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**197**	**17**	9%	**17**	9%	**17**	9%	**197**	100%	**14**	7%	**197**	100%	**0**	0%

The OIG numbers reported for the above measures were significantly different. In particular, the OIG reported 258 total systems, of which no systems had completed security plans and no systems had been fully certified and accredited. The Department reports that it has established an Office of Information Technology Security in the Office of the Chief Information Officer. This office is staffed with certified security professionals, professional trainers, and project managers. In addition, the Department states that they are currently conducting an annual awareness and training program including an introduction to security principles and practices and reinforces existing policy and procedures as they relate to accessing and using federal IT resources.

Responsibilities of Agency Head

The Department reports that HUD's Assistant Secretary for Administration/Chief Information Officer has established a Senior Agency Security Managers' Advisory Counsel from the program offices to carry out security policy compliance, risk management, contingency planning, certification, training and capital planning to meet FISMA requirements. The Chief Technology Officer (CTO) oversees the security of IT systems and data. The HUD Chief Information Security Officer (CISO) is responsible for ensuring that information security decisions are based on cost, risk, and mission impact, including tracking investments to make certain that security weaknesses are budgeted for, and corrective action plans are approved prior to adding new system features. The CISO reports directly to the CTO. The CISO has responsibility for ensuring that the HUD IT Security Program is in compliance with federal information security laws and directives, and that security life cycle management is integrated in all aspects of HUD's IT process. The CISO is also responsible for development and execution of HUD's Information Security Five-Year Strategic Plan.

Department of Interior

IT Security Background

DOI reported twelve programs at twelve bureaus, supported by 164 systems and 80 contractor operations and facilities. Eleven programs, 80 systems, and eight contractor operations were reviewed as part of this report. The Department used NIST self-assessment guidance to review its programs, systems and contractor operations. Various bureaus are in different stages of completing a systems inventory. Fifteen material weaknesses were reported by the Department, of which thirteen were repeated from last year. Causes of material weaknesses varied including inadequate security documentation, lack of accreditation, and non-compliance with DOI and NIST contingency planning guidance. All material weaknesses related to IT security were included in POA&Ms. 241,304 incidents were reported, of which 68 were reported externally to FedCIRC or law enforcement. DOI reported 96% of all operational systems integrated security costs into the life cycle of the system.

Management and Program Performance Highlights Reported by the Department

- 97% of all agency employees and 81% of employees with significant security responsibility have received IT security training. Training included CIO sponsored classes to prepare IT security staffs for Certified Information Systems Security Professionals examinations.

Management and Program Performance Highlights Reported by the OIG

- DOI has deployed an automated self-assessment tool that complies with NIST standards.
- Senior management focus on IT security is sustained, and the agency head has institutionalized IT security as a priority through organizational changes and standardization of security functions. This focus permeates through most DOI bureaus and senior level management, and includes the CIO.

Management and Program Performance Challenges Reported by the Department

- Around half of all systems have been assessed for risk and have IT security plans, and 10% of Department operational systems have completed certification and accreditation.
- Translating and implementing all security policies, procedures and plans into varied operational environments so as to avoid competing priorities and ineffective management of an enterprise-wide security program.

Management and Program Performance Challenges Reported by the OIG

- The Department's POA&M process has major shortcomings including a lack of complete POA&Ms for all systems, inadequate integration of security weaknesses to system budget requests, and inappropriate prioritization of weaknesses.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Interior FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**164**	**71**	43.3%	**87**	53%	**17**	10%	**158**	96%	**99**	60%	**56**	34%	**32**	20%

The Department reported the CIO manages and oversees the activities of component CIOs, meeting monthly with each of them to discuss component security status and performance. Component CIOs must submit formal project plans that address how they will comply with Department security policy and guidance. Based on this information, the CIO publishes scorecards for each bureau that monitors nine major performance elements. The scorecards are then presented to senior management and play a critical role in establishing executive accountability. The Department reports that the CIO established an IT security awareness training program for all DOI employees and contractors that provides a basic understanding of IT security issues, and is developing more specialized training options for employees with significant security responsibilities.

Responsibilities of Agency Head

The Department reported the agency head delegated authority to the CIO to establish and enforce DOI-wide information system security policies and procedures. The agency head is the designated approving authority for all systems, along with program heads and appropriate assistant secretaries who also act as the designated approving authority for their respective systems. Additionally, the CIO reviews and approves all major IT investments. The agency head moved the CIO's position to the immediate Office of the Secretary and included the CIO in DOI's senior management councils, empowering the CIO with authority to enforce Department IT security policies and procedures. The OIG reported that the Department has not integrated the IT security program with its critical infrastructure protection responsibilities, however, the DOI IT security manager does coordinate with the newly created Office of Law Enforcement and Security – which carries out critical infrastructure responsibilities. Additionally, the Department does not have consistent policies and procedures so as to prevent unnecessary duplication of efforts and security inconsistencies. The Department reports mission and national critical operations and assets have not been fully identified. DOI established a centralized computer security incident reporting capability and developed a computer security response handbook. The Department reports components report directly to FedCIRC and share incident information across the Department. The Department has not developed configuration requirements.

Department of Justice

IT Security Background

DOJ reported 253 systems, 24 programs, and 35 contractor operations and facilities. All programs and 206 (or 81%) Department systems were reviewed for this report. While only half of contractor operations and facilities were reviewed, DOJ IT security requirements are incorporated into contracts and penetration tests and audits assess the adherence of contractors to provisions in the contracts. Two material weaknesses were reported, one of which is a Department level material weakness relating to component implementation of IT security controls. Both material weaknesses are repeated from the previous year and have associated POA&Ms to manage corrective action. DOJ reported 133,577 security incidents of which 51 were reported to FedCIRC. Seven incidents were reported externally to law enforcement. Eighty-six percent of all operational systems integrated security control costs into system life cycle.

Management and Program Performance Highlights Reported by Department

- DOJ integrates IT security costs throughout most operational system's life cycle.
- DOJ implemented a web-based security awareness training program for a large part of the Department. This web-based application allows users to tailor the content and scheduling of training modules depending on personnel roles and responsibilities, and tracks and reports employee progress.
- DOJ is developing a security architecture consistent and integrated with the Department's overall enterprise architecture. This effort allows DOJ to better identify crosscutting security needs and leverage common solutions while also standardizing security policy and practices throughout the enterprise.

Management and Program Performance Challenges Reported by Department

- OIG reports two material weaknesses in FY03, one resulting from a Department-wide finding of overall poor IT security control implementation and the other one for the FBI's computer security program. Both material weaknesses were repeated from last year.
- DOJ has not fully identified its national critical and mission critical operations and assets, or the interdependencies and interrelationships they have with one another.

Management and Program Performance Challenges Reported by the OIG

- The POA&M process is weak in all areas, in particular POA&Ms were not used to monitor component adherence to Department policies and procedures, and some corrective actions were not verified.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Justice FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**255**	**229**	90%	**220**	86%	**202**	79%	**220**	86%	**197**	77%	**196**	77%	**80**	31%

The Department reports that the enterprise-wide responsibility for ensuring security of IT rests with the CIO. The CIO established an IT security office to oversee the implementation of the Department's security program, led by the chief information security officer. Additionally, the office is responsible for developing policy and standards, and has organized a security council comprised of top security officials from each of Justice's component organizations. The Department reports the CIO reviews security policy and verifies weaknesses found from testing and auditing are appropriately handled and addressed in a centralized database. While only 77% of all employees have received security awareness training, the Department recently implemented a web-based training tool. The tool will provide training for all employees and contractor personnel on a regular basis.

Responsibilities of Agency Head

The Department reports that major components are directed to implement an IT investment management process that would include IT security policy. According to the Department, the OCIO also controls phased review and provides the CIO with information regarding the status of each major investment to identify problem areas. The OIG reports no major IT investment decision can be made without the CIO's review and concurrence. The Department reports that program managers are responsible for integrating and maintaining IT security controls throughout the system life cycle and that the Department head reviews results of security evaluations of each component with the CIO. The Department continues to develop a security architecture as an integrated element of the Department EA, so that the IT investment process adequately incorporates security needs. The Department reported that the IT security staff coordinates with other security programs, including personnel and physical security. All Department policies are coordinated through the Assistant Attorney General to ensure consistency and clear articulation. While the Department has identified some essential infrastructure, full identification of mission and national critical operations and assets has not been completed. The DOJ Computer Emergency Response Team (DOJCERT) has developed standards for reporting incidents within the Department and serves as the single point of contact to FedCIRC and verifies patch implementation at components.

Department of Labor

IT Security Background

DOL reported 81 systems supporting thirteen programs housed at thirteen bureaus and eleven additional contractor operations and facilities. The Department reviewed all programs, 77 systems, and 10 contractor operations using the NIST self-assessment guide, audits and inspections, among other evaluations. Zero material weaknesses were reported by the Department. The Department reported a total of 76 incidents, of which zero were shared externally to FedCIRC. Eighty-nine percent of all operational systems integrated IT security control costs into the life cycle of the system.

Management and Program Performance Highlights Reported by Department

- DOL maintains a high percentage of security awareness and training for employees, including all employees with significant security responsibilities.
- DOL ensures IT security issues are addressed and investments meet high security performance throughout system life-cycle by integrating the results of risk-assessments into the capital planning and investment control process.

Management and Program Performance Highlights Reported by the OIG

- DOL effectively manages a Department-wide POA&M process to address IT security weaknesses.

Management and Program Performance Challenges Reported by the OIG

- Risk assessments using the NIST Special Publication 800-26 as guidance were not conducted for eight of eleven systems evaluated by the OIG.
- While DOL is working to fully certify and accredit all systems, none of the systems in the OIG sample subset had performed a full certification and accreditation that included testing of the critical controls identified by management.
- DOL incident handling capability has not been fully implemented at two components and review discovered bureaus where applications were lacking required software patches as recommended by FedCIRC.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Labor FY2003 FISMA Report															
	Total Number of Systems	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**81**	**75**	93%	**77**	96%	**47**	58%	**72**	89%	**59**	72%	**75**	90%	**36**	44%

DOL reports continued progress in improving IT security performance. The Department reports the CIO has established a Department-wide IT security program, supported by an agency information security officer. Additionally, the CIO monitors and evaluates the performance of all bureaus on a quarterly basis, and monitors the integration of security into the lifecycle of Department systems and investments. Reviews include the results and status of certifications and accreditations, as well as other evaluations and audits. The OIG reports that the majority of security weaknesses are included in Department POA&Ms. DOL reports 87% of employees with significant security responsibilities received specialized security training, and 96% of all Department employees received security awareness training.

Responsibilities of Agency Head

The Department reported that the agency head has delegated to the CIO and senior information security officer roles and responsibilities under FISMA, but reserves final decision making authority. Additionally, the Department head sponsored the establishment of the Management Review Board and a Technical Review Board to help evaluate and make decisions on Department IT investments and promulgate a system development life cycle management manual. A Security Officer's Working Group regularly convenes to discuss various IT security issues the Department faces. The cyber security program coordinates with DOL's critical infrastructure protection responsibilities, including development of contingency plans. Separate staffs coordinate with the Office of the Assistant Secretary for Administration & Management to prevent inconsistent physical and cyber security policy and procedures. The Department reported that DOL does not have any national critical operations and assets, and has identified mission critical operations and assets. Additionally, the interrelationships of mission critical operations and assets are fully identified, and as a result continuity of operations plans appropriately prioritize essential functions. Department policy outlines how all IT security incidents are to be reported, and the timeliness of incident reporting follows escalation procedures depending on incident severity. The Department reported system administrators are responsible for verifying and reporting the completion of patch installation, and DOL develops configuration requirements to address effective patching of known vulnerabilities.

National Aeronautics and Space Administration

IT Security Background

NASA reported 11 centers, 1,555 systems, and 232 contractor operations and facilities. NASA reviewed two programs and 1,297 systems as part of their annual review, and none of the 232 contractor operations and assets. Almost all (99%) operational systems integrated security costs into the system life cycle. NASA reported the overall IT security program as a material weakness based upon numerous weaknesses, many of which were repeated findings from the previous year. A total of 113 security incidents were reported, all of which were reported to FedCIRC and external law enforcement.

Management and Program Performance Highlights Reported by Agency

- Ninety-eight percent of 1,555 systems are certified and accredited.
- While the OIG found inconsistent interpretation of NASA IT security policy at some components, the agency has introduced a one-NASA IT governance model that helps ensure IT security program weaknesses are appropriately addressed in a timely manner in adherence to agency security policies and procedures. Centralized governance has also developed appropriate consequences for policy noncompliance.
- IT security costs are integrated into the system life cycle of almost all operational systems, including new system development and major upgrades.

Management and Program Performance Challenges Reported by the OIG

- Areas of the POA&M process needing improvement included better integration of agency program officials in managing POA&MS, more complete accounting of security weaknesses discovered during audits and reviews, better integration of security funding in the agency budget, and more appropriate prioritization of security weaknesses.
- NASA has not fully identified national critical and mission critical operations and assets as well as their interrelationships and interdependencies.
- Records from the NASA Incident Response Center lacked information on when incidents occurred and when they were reported to FedCIRC, and some Centers did not report all security incidents.

Responsibility of Agency Program Officials and CIO

Table C.1 of the National Aeronautics and Space Administration FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**1555**	**1516**	97%	**1297**	83%	**1520**	98%	**1547**	99%	**1292**	83%	**1471**	95%	**1302**	84%

The agency reports the CIO centrally manages an agency-wide IT security program and regularly evaluates component security performance thru established reporting processes and third party reviews. Agency POA&Ms identify and monitor most security weaknesses. The agency reports NASA provided IT security awareness training for 98% of their employees, and 99% of those employees with significant security responsibilities received specialized security training. While the OIG found areas where technical training could be improved, the training did include a number of on-line options as well as three on-site security courses at different locations throughout the agency. The OIG reported systems administrators lack proper security training and the agency reports initiating a certification program to ensure they receive adequate security training.

Responsibilities of Agency Head

The agency reports that the agency head sponsors a security scorecard at each Center to monitor and grade Center adherence to agency security policies and procedures. This reporting helps ensure security policy and guidance is practiced throughout the life-cycle of each system, however, the OIG reports inadequate or incomplete implementation of NASA's computer security policies for some mission critical assets. The agency reports major operating components within the agency can not make IT investment decisions without the concurrence of the OCIO. The agency head established a third party review process to verify adherence to agency security policies at two major operating components. The agency reports that the Deputy CIO for IT Security coordinates with the Office of Security Management and Safeguards (OSMS) to protect the agency's critical infrastructure, and the OCIO is responsible for operations and execution of the agency's IT security program. During critical infrastructure review, NASA conducts vulnerability risk assessments to identify weaknesses and develop mitigation strategies. The agency reports NASA's incident response center works with FedCIRC and the OIG to report security incidents and disseminate alerts, and that NASA components share incident information within two hours of incident confirmation. Additionally, the agency reports system administrators are ultimately responsible for finding and applying necessary patches and for developing specific configuration requirements for operating systems and requirements to address continuous patching of security vulnerabilities.

National Science Foundation

IT Security Background

NSF reported one program, 19 major applications and support systems, and one contractor operation. NSF's program and contractor operations and facilities were reviewed as part of this report, as well as 18 major applications and support systems. Reviews were conducted based on NIST's Guide for the Certification and Accreditation of Federal Information Systems. The OIG reported three material weaknesses, of which none were repeated from last year. These weaknesses were integrated into agency POA&Ms. NSF identified eight security incidents; six were reported to FedCIRC and one to external law enforcement. NSF reports all operational systems integrated security control costs into the system life cycle.

Management and Program Performance Highlights Reported by Agency

- NSF has strengthened the central management of the IT security function by establishing and filling the position of Chief Information Security Officer.
- Both the CIO and CISO meet monthly with an agency Security Working Group to discuss cross-cutting agency information security issues. The Security Working Group is comprised of senior representatives from directorates and addresses policies, procedures, and plans related to information, physical, and personnel security.

Management and Program Performance Highlights Reported by the OIG

- NSF OIG verifies existence of agency POA&M process and the CIO reviews a report of POA&M actions and progress on a weekly basis.

Management and Program Performance Challenges Reported by the OIG

- While configuration requirements address patching of vulnerabilities, the agency's patch management process has not been implemented agency-wide, leaving some system vulnerabilities and some patches not tested in a timely manner.
- Formal information security policies and procedures have not yet been implemented at the U.S. Antarctic Program.
- While the process of certification and accreditation has improved, and 95% of all systems have completed certifications and accreditations, some shortcomings exist. Improvements would include more thorough documentation of system interconnectivity and controls and increased testing of these controls.

Responsibility of Agency Program Officials and CIO

Table C.1 of National Science Foundation FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**19**	**19**	100%	**18**	95%	**18**	95%	**19**	100%	**18**	95%	**16**	84%	**15**	79%

The agency reports the CIO centrally manages the agency's IT security program, and evaluates compliance with agency polices and procedures. NSF has published and disseminated an agency Information Security Handbook that provides an overview of the agency's information security program and identifies key roles and responsibilities. The CIO meets monthly with a security working group, and ensures weaknesses in the POA&M are tracked in an automated database containing action items, responsibilities, and targeted dates for completion of corrective action. Additionally, the CIO regularly discusses relevant security topics at agency executive meetings. The agency reports recurring penetration testing and vulnerability scanning helps identify weaknesses in implementation of security policies and procedures. The OIG reports 84% of agency employees have received IT security awareness training and 83% of employees with significant security responsibility received specialized security training.

Responsibilities of Agency Head

The agency reports that the agency head has delegated to the CIO the primary responsibility for development and maintenance of the NSF Information Security Program, and participates in monthly project reviews to ensure security requirements are addressed throughout the system lifecycle. Agency components must receive OCIO concurrence prior to making major investment decisions. The OIG reports the agency head reviews security objectives during annual system security reviews, and evaluates the progress of security requirement implementation through periodic management reviews with the CIO and the Senior Management Integration Group – a group chaired by the agency head and comprised of Assistant Directors, Office Directors, and other agency executives. The OIG reports NSF has a single, integrated security program to protect critical infrastructure to coordinate IT security and physical security efforts. NSF does not have national critical operations and assets and has identified mission critical operations and assets, as well as their interdependencies and interrelationships. The agency reported one agency component, NSF's Computer Incident Response Team, communicates directly with FedCIRC, and the OIG is responsible for reporting externally to law enforcement. The agency performs periodic scans and penetration testing to detect vulnerabilities.

Nuclear Regulatory Commission

IT Security Background

NRC reported 20 systems, 1 program, and 7 contractor operations and facilities, all of which were reviewed for this report. No material weaknesses were reported. NRC reported 67,626 security incidents, all of which were reported to FedCIRC. Zero incidents were reported externally to law enforcement. According to the Commission's report, 100% percent of all operational systems integrated security control costs into system life cycle.

Management and Program Performance Highlights Reported by the Commission:

- NRC established policies addressing mandated security documents for major applications, an NRC automated information systems security program and recurring NRC security tasks throughout the systems development life cycle.
- NRC has integrated security control costs into the systems development life cycle for 100% of their systems.
- The NRC updated its patch management policy guidance in FY 2003. The process is managed by the network infrastructure security team, working closely with the systems administrators for all the NRC systems. Critical patches that have been identified by FedCIRC are installed, and the network infrastructure ISSO confirms that systems administrators have installed the patches.

Management and Program Performance Challenges Reported by the OIG

- The Operating and System Software Maintenance Procedures are not followed consistently, contributing to an incomplete inventory of NRC operating and system software. Subsequently, commission leaders may not be able to identify all systems operating on a particular type or version of software and when they may need a patch to counter a vulnerability or threat.
- Review of quarterly POAM reports and the Information Technology Security Tracking Systems (ITSSTS), reveal that new weaknesses and corrective actions identified during the past fiscal year were not always incorporated into these management tools.
- The NRC master inventory of systems needs improvement, as limited segments of the NRC IT infrastructure are being examined. Those systems that are being examined do not always indicate the internal and external system interfaces.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Nuclear Regulatory Commission FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**20**	**20**	100%	**18**	90%	**18**	90%	**20**	100%	**18**	90%	**18**	90%	**17**	85%

The Commission reports that the CIO is responsible for managing the agency-wide automated information security program. In turn, the CIO assigned the Senior Information Technology Security Officer (SITSO) with the task of exercising day to day management and oversight of the commission's security program. The agency-wide automated information security program management directive outlines the responsibilities and authority of all other senior agency officials in the context of IT security. The Executive Director of Operations (EDO) and CIO then conduct reviews of the NRC program and individual system and submit quarterly corrective POA&M's to OMB to promote the implementation and enforcement of the NRC automated information security program.

Responsibilities of Agency Head

As stated in the Commission's report, the NRC's most senior leader, the EDO, supervises the CIO and all IT program officials. Furthermore, the agency head is obligated to ensure that all requirements of the NRC automated information security program are being implemented and enforced. The agency head, along with the CIO, meet this objective by focusing on the performance measures for the program, guaranteeing that monthly progress reports are filed with each Commission office and ensuring that all elements of the NRC automated information security program are being supported. The EDO manages these tasks by using a central tracking system to follow all system information, and ensures that all components have documented and reported security incidents by having the agency act in compliance with FedCIRC security incident policies. The Computer Security Incident Response Capability team and the NRC Office of the Inspector General collaborate with one another when an incident requires the involvement of law officials.

Office of Personnel Management

IT Security Background

OPM reported six programs, 45 systems and four contractor operations and facilities housed at six bureaus. The OIG did not identify material weaknesses for the second straight year. Sixteen major or sensitive systems were reviewed by the agency over the past year. OPM's system inventory of 45 total systems is being updated to reflect findings from an upcoming agency effort to identify remaining systems. Forty percent (18 of 45) of all operational systems integrated security costs into the life cycle of the system.

Management and Program Performance Highlights Reported by the Agency

- Over 91% of all systems have been assigned a level of risk, have up-to-date security plans, tested and evaluated security controls, and are certified and accredited.
- Agency officials have developed IT security policy applicable agency-wide, including guidance and definitions to address security control elements aligned to OMB and NIST guidance.

Management and Program Performance Highlights Reported by the OIG

- OPM has developed, implemented, and is effectively managing an agency-wide POA&M process, although some weaknesses were not adequately included in the POA&M process.

Management and Program Performance Challenges Reported by the Agency

- The majority of agency systems (60%) do not include security costs in the system life cycle.

Management and Program Performance Challenges Reported by the OIG

- While controls are in place to identify, prioritize, and protect operations and assets within OPM's enterprise architecture, not all program officers have completed business recovery plans that identify and document processes and resources necessary to support OPM's mission essential functions.
- Not all incident reports are completed according to OPM's Incident Response and Reporting Procedures document.

Responsibilities of Agency Program Officials and CIO

Table C.1 of the Office of Personnel Management FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**45**	**41**	91%	**41**	91%	**41**	91%	**18**	40%	**41**	91%	**16**	36%	**7**	16%

The above numbers reflect the results of the OCIO review and while generally consistent with the OIG's findings, the OIG reported slightly fewer systems had risk assessments, integrated security costs into system life cycle, and security controls tested and evaluated in the last year as well as slightly more systems operating with complete certification and accreditation. The agency reports the CIO manages the agency IT security program, but agency officials have not fully complied with program policies. To better facilitate compliance, the CIO has developed implementation guidance to assist program offices in identifying and narrowing expectation gaps. Additionally, the CIO uses the agency POA&M and results of system assessments to track security program compliance, and has appointed a senior agency information security officer. OPM is unable to identify the number of employees who have received security awareness training, and half of agency employees with significant security responsibility received specialized training.

Responsibilities of the Agency Head

The agency reported the OPM Director and Deputy Director delegated accrediting authority for all systems to Associate Directors and Heads of Offices. The Director delegated the CIO to review and approve all major IT investment decisions, and the agency has implemented a standardized system development life cycle management process. The agency reports all major IT investment decisions must receive CIO concurrence. The Director has also delegated IT security responsibilities to the CIO, and sponsors the IT Security Guide to promulgate agency security policies and responsibilities. The agency reports separate staffs are devoted to IT security and physical security, and their responsibilities are clearly delineated to avoid duplication and overhead costs. The agency has fully identified mission and national critical operations and assets as well as their interdependencies and interrelationships. The agency reports configuration requirements have been developed, and the requirements include patching.

Small Business Administration

IT Security Background

SBA reported seven programs, 38 systems, and five contractor operations. SBA's FISMA review included all programs, 35 systems, and four of their contractor operations and facilities, and the OIG evaluation reviewed 37 systems and three contractor operations and assets. The OCIO reported five material weaknesses for the agency's IT systems, of which four were repeated from FY02. Over 169,000 incidents were reported, all of which were reported to FedCIRC. Only thirteen percent (5 of 38) of SBA's systems integrated security costs into the system life cycle.

Management and Program Performance Highlights Reported by the Department

- SBA continued to make improvement in the overall percentage of systems with certifications and accreditations from 65% in FY02 to 74% in FY03.
- The Information Security Office has begun using the INFOSEC Management Database to track POA&M data, allowing system reports to be provided to system owners who then directly update status of system weaknesses.
- SBA's Automated Information System Security Program Policy Document establishes agency roles, policies, and procedures for ensuring adequate security of information resources.

Management and Program Performance Challenges Reported by the OIG

- SBA has not yet developed an agency-wide integrated security plan to manage the agency's IT security program across all systems and field offices. Completion of the plan will allow for full identification of system interdependencies and interrelationships and integration of security considerations throughout the capital planning and investment process.
- Computer intrusion detection capabilities were identified as a material weakness.
- SBA has developed and implemented a POA&M process, but not all weaknesses are included in the POA&M, some weaknesses recorded as closed remain uncorrected, and weaknesses are not appropriately prioritized.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Small Business Administration FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**38**	**28**	73%	**28**	73%	**28**	73%	**5**	13%	**7**	18%	**15**	38%	**15**	38%

While the OCIO and OIG generally reported the same quantities for the above performance measures, the OIG identified no systems as having security control costs integrated into the system life cycle. The agency reports the CIO uses the development of system self-assessments and certification and accreditation process to ensure SBA's geographically spread out bureaus comply with the agency-wide IT security program objectives. Furthermore, the CIO conducts periodic audits and evaluations to assess bureau progress in implementing IT security policy. Computer based security awareness training is required annually, and program managers, security officers, and system administrators receive additional training. The agency reports 91% of agency employees received IT security training this past fiscal year, as did 78% of employees with significant IT security responsibilities.

Responsibilities of Agency Head

The agency reported the agency head reviews security plans during the certification and accreditation process, while a Chief Infrastructure Assurance Officer appointed by the agency head integrates the security program with critical infrastructure protection priorities. Additionally, a major operating component of the agency cannot make significant IT investment decisions without review and concurrence of the Business Technology Investment Council. The Council is comprised of senior agency executives and chaired by the CIO and works to review and identify effective IT solutions for the agency in support of the agency's mission, infrastructure, and standards. Consistent policies and procedures between the agency's Facilities Office and IT security program eliminate duplicative overhead costs that ensure separate staffs complement policies and procedures across various programs and functions. The OIG reports SBA has fully identified national and mission critical operations and assets, and work remains to fully identify interdependencies and interrelationships of these assets and operations. SBA is developing an agency Critical Infrastructure Protection Plan for cyber systems and physical assets. The agency reports that the agency head has delegated reporting of IT security incidents to the CIO and agency Computer Security Program Manager. Additionally, the OCIO has issued a Computer Emergency Response Team procedures manual to report and respond to IT security incidents, and established a line of communication between the IT Security Office and FedCIRC to report incidents. While

no incident required immediate reporting to FedCIRC in the past year, all incidents were reported on a monthly basis. Patches are installed and tested upon distribution and system specific configuration requirements are developed and complied, including the capability to patch uncovered security vulnerabilities.

Social Security Administration

IT Security Background

SSA reported 65 programs, 17 systems, and 16 contractor operations and facilities. The agency reports all systems and contractor operations were reviewed in FY03, as well as thirty SSA programs. SSA reported no material weaknesses. The agency is updating its system inventory which currently accounts for 90% of all of SSA's systems. The agency reports it adequately integrated system security provisions into each of its data exchange agreements with human service agencies across the country, and these provisions are consistent with NIST guidance and include onsite visits to ensure security requirements are enforced. SSA reported that all operational systems integrated security costs and considerations into their system life cycle.

Management and Program Performance Highlights Reported by Department

- All significant systems are risk assessed, have documented IT security plans, have been tested and evaluated, and are certified and accredited.
- Almost 100% of agency employees have received IT security awareness training, and security officers are required to receive 16 supplemental hours of IT security training per year.
- The agency head has integrated responsibility for IT security management and critical infrastructure protection into job performance standards for agency senior executives.

Management and Program Performance Challenges Reported by Department

- SSA is conducting a complete system inventory to ensure all agency systems have been identified.
- Establish a better process to determine that configuration standards remain consistently enforced.

Management and Program Performance Challenges Reported by OIG

- The agency POA&M process was not verified by the OIG due to inconsistent practices to develop POA&Ms, inadequate access to POA&Ms by OIG, and lack of POA&Ms accounting for all known IT security weaknesses. In order to optimize the agency POA&Ms, a consolidated database is being developed to track only IT security weaknesses.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Social Security Administration FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**17**	**17**	100%	**17**	100%	**17**	100%	**17**	100%	**17**	100%	**16**	94%	**14**	82.4 %

The agency reports that the CIO has implemented an agency wide IT Security Program, and the chief security officer reports directly to the CIO to provide governance of the IT Security Program. Additionally, the CIO and agency management is notified of weaknesses discovered during audits and evaluations and is updated on completed corrective actions on a quarterly basis. The chief security officer also ensures external systems maintain adequate IT security provisions, develops and implements IT security policy, and evaluates compliance to policies and procedures for all systems. The agency reports over 99% of all agency employees have received IT security awareness training, and 76% of those employees with significant IT security responsibilities have received specialized security training.

Responsibilities of Agency Head

The Commissioner has established the OCIO at the Deputy Commissioner level, and as a result, the CIO is directly responsible to the Commissioner for developing and maintaining the agency wide IT Security Program. The agency reports major operating components can not make major IT investment decisions without the concurrence of the CIO, and the Executive IT Capital Investment Board reviews proposed acquisition of new IT. The agency has integrated the IT security program with critical infrastructure protection responsibilities, and the agency has separate staffs devoted to physical and personnel security programs so as to avoid duplication of security costs and ensure consistency of security polices and procedures. The OIG reports that SSA has fully identified mission and national critical operations and assets, and is working to fully identify the interdependencies and interrelationships between them. The agency reports incident handling and response resolution are centrally managed, including the testing and certifying of new patches prior to deployment. Additionally, SSA has developed configuration standards and an automated process is in place to identify configuration anomalies and discrepancies.

Department of State

IT Security Background

The Department reported 33 programs, 139 systems, 26 contractor operations and facilities, and 293 sites. The Department used NIST self-assessment guidance to review all programs and contractor operations and facilities, but only fifty systems were reviewed and no sites were reviewed. The OIG reported one material weakness caused by a lack of internal controls in regards to system security pertaining to the Department's financial management system. The material weakness was repeated from last year. The Department did not report integration of FY03 IT security costs into the system life cycle, but did demonstrate integration as part of the FY05 budget process. Nineteen incidents were reported, of which eight were reported externally to FedCIRC.

Management and Program Performance Highlights Reported by Department

- The Department appointed a Chief Information Security Officer who reports directly to the CIO and leads the Office of Information Assurance for the entire Department.
- All Department systems have been assessed and assigned a level of risk.

Management and Program Performance Highlights Reported by OIG

- The OIG reports that the CIO issued the information assurance performance measures plan and asked all bureaus and missions to implement procedures for collecting and submitting IT security data in accordance with the plan. The data is fed into an automated workbook in which all requirements are reported.

Management and Program Performance Challenges Reported by Department

- While the Department is progressing thru an 18-month accreditation plan for operational systems, thirty-six percent of Department systems operate with complete certifications and accreditations.
- Security control costs are not identified throughout the system life-cycle.

Management and Program Performance Challenges Reported by OIG

- Agency officials do not have appropriate methods in place to ensure contractor provided services are adequately secure, and work remains to solidify the agency's system inventory.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of State FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**139**	**139**	100%	**51**	37%	**50**	36%	no response	no response	**46**	33%	**41**	29%	**50**	36%

The OIG reports the CIO has established the Department's information security program and evaluates the performance of all bureaus through an automated reporting tool to track compliance with agency IT security measures. A senior information security officer was appointed to direct the Office of Information Assurance and the Department's Information Security program. The OIG reports that POA&Ms do not address all known security weaknesses. Roughly half (45%) of all employees have received IT security awareness training. While the Department's FISMA report identified the total number of employees with significant IT security responsibilities, it did not identify the percent of employees who had received specialized training.

Responsibilities of Agency Head

The Department reported that the Under Secretary for Management issued a Memorandum to all Under Secretaries and Assistant Secretaries informing them of their responsibility to ensure the security of all information under their purview. Major operating components can make investment decisions without the concurrence of the CIO, but the CIO is part of the E-Gov Program Board to review all major IT investment proposals. The CIO has designated the chief information security officer (CISO) as responsible for leading the Office of Information Assurance and the Department's Information Security program. One of the CISO's first tasks is to develop an IT security program management plan. The Department reported that the Under Secretary for Management, on behalf of the Secretary sponsored development of a systems authorization plan headed by the CISO. The Department is integrating IT security responsibilities and policies with critical infrastructure responsibilities, and the Bureau of Diplomatic Security is responsible for personnel and physical security. The Department reports all mission and national critical operations and assets or their interdependencies and interrelationships have not yet been identified. The Computer Incident Response Team (CIRT) serves as the Department's focal point for reporting IT security incidents, and directly communicates with FedCIRC. The Department developed and complied with specific configuration requirements, and these requirements address patching of known IT security vulnerabilities.

Department of Transportation

IT Security Background

DOT reported 630 systems, 12 programs, and 36 contractor operations and facilities. Thirty-three contractor operations (or 92%), 366 (or 58%) Department systems and all programs were reviewed for this report. One material weakness was reported, identifying the Department's IT security program as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA). DOT reported 69 security incidents of which 17 were reported to FedCIRC. One incident was reported externally to law enforcement. Sixty-six percent of all operational systems integrated security control costs into system life cycle.

Management and Program Performance Highlights Reported by the Department

- DOT established a Department wide security incident response center. This center, with the cooperation of FAA's incident response center, detects, analyzes, and prevents hundreds of potential intrusions from the internet on a daily basis.
- DOT provided Department wide security awareness training to 100% of more than 60,000 employees, and specialized training in areas such as network security to over 600 employees.

Management and Program Performance Highlights Reported by the OIG

- The OIG reported that DOT developed a more reliable inventory of systems in response to recommendations from the FY02 FISMA report.

Management and Program Performance Challenges Reported by the Department

- Thirty-three percent of DOT's systems had been certified and accredited.

Management and Program Performance Challenges Reported by the OIG

- DOT's IT security program has been reported as a material weakness under FMFIA due to lack of investment criteria for IT investments, accurate cost estimates, and inadequate business impact analysis.
- DOT has developed and tested contingency plans for only 16% systems. The OIG states that without contingency planning and analysis, management does not know how long business operations could continue without computer systems support.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Transportation FY2003 FISMA Report															
	Total Number of Systems	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested***	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**630**	**378**	60%	**286**	45%	**209**	33%	**415**	66%	**328**	52%	**167**	27%	**103**	16%

During 2003, DOT appointed a Department wide CIO. Although the CIO does not have authority to approve Operating Administration IT budgets or provide input to the Operating Administrations' CIO performance appraisals, the Department wide CIO's responsibilities were increased through the formation of the Departmental Investment Review Board. The Board, chaired by the Deputy Secretary, with the CIO, the Chief Financial Office, the General Counsel, and the Assistant Secretary for Administration as official members designated by the Secretary, has the authority to approve, modify, or terminate major IT investments.

Responsibilities of Agency Head

The Secretary has delegated the responsibilities for developing and maintaining DOT's information security program and overseeing program officials' performance in practicing information security to the CIO. The CIO office has issued multiple implementation guidelines, including methodology to certify system security throughout the lifecycles of individual systems. Additionally, the CIO's Office conducted compliance reviews on the Operating Administrations' progress in developing IT security plans and certifying systems for meeting requirements.

Department of the Treasury

IT Security Background

Treasury reported 60 programs, 708 systems and 39 contractor operations and facilities contained in thirteen bureaus. The Department reviewed 57%, 23%, and 90% of these programs and assets, respectively. The Office of the Chief Information Officer (OCIO) reported seven material weaknesses for the Department's IT systems, five repeated from FY02. Over 16 million incidents were reported, with some bureaus reporting zero incidents and others in the millions. FedCIRC received incident reports on less than one percent of them. Only 29% (203 of 708) of Treasury's systems integrated security costs into the life cycle of the system.

Management and Performance Highlights Reported by the Department

- The Department finalized and distributed an IT security policy, the Treasury Information Technology Security Program, containing Treasury's updated security policies.
- A FISMA Compliance Working Group has been established which includes representatives from all bureaus, to focus on common challenges and solutions to improve FISMA compliance.

Management and Performance Highlights Reported by the OIG

- The Office of the CIO developed the Treasury Information System Tracker (TIST) database to inventory all Treasury information systems.

Management and Program Performance Challenges Reported by the Department

- The percentage of certified and accredited operational systems decreased over the last year and remains low.

Management and Program Performance Challenges Reported by the OIG

- A small portion of programs and systems were reviewed and the Department did not use NIST guidance for all reviews.
- Deficiencies in the Department's POA&M process exist. In some instances, POA&MS were not developed or systems did not include all weaknesses, program officials did not report on a regular basis, and weaknesses were inappropriately prioritized.

Responsibilities of Agency Program Officials and CIO

Table C.1 of the Department of Treasury FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level or risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested**	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**708**	**304**	43%	**304**	43%	**172**	24%	**203**	29%	**156**	22%	**315**	45%	**291**	41%

The Department reports the CIO is the senior official responsible for all aspects of IT security implementation and oversight. Additionally, the CIO executes IT security duties through the Office of Security Compliance (OSC) which is the Department's main mechanism for enforcing IT security requirements, policies and procedures. During FY03, the OSC activities included conducting program and system reviews, assisting bureaus with the development of POA&Ms, monitoring mitigation of identified weaknesses, conducting contractor facility reviews, and executing an outreach initiative to help bureaus implement all aspects of FISMA. The Department report states 77% of all employees received IT security awareness training and 72% of Department employees with significant IT security responsibilities received specialized training. The OCIO helps sponsor an IT Security Training Forum, which meets quarterly to discuss IT security training best practices.

Responsibilities of the Agency Head

According to the Department report, the Treasury Secretary delegated responsibility and authority for FISMA implementation to the Department's Assistant Secretary for Management/Chief Financial Officer, which was further delegated to the CIO. Additionally, a consolidated IT and physical security staff serves under the Assistant Secretary for Management/Chief Financial Officer. A memorandum required bureau CIOs to oversee the performance of their program officials to verify that IT security plans are up-to-date and practiced throughout the enterprise. The Secretary works to ensure the Department's information security plan and procedures are practiced throughout the lifecycle of each system by utilizing annual self-assessments for each IT system. While the Department has fully identified national and mission critical operations and assets, it has not yet identified their interrelationships and interdependencies. The Treasury Computer Security Incident Response Center centrally manages response centers at each bureau, and the OIG reported configuration requirements were not developed.

Department of Veterans Affairs

IT Security Background

VA reported 871 systems, 24 programs, and 127 contractor operations and facilities. All Department programs and systems were reviewed for this report. Eighty-one (or 64%) contractor operations and facilities were reviewed. Five material weaknesses were reported, and all five related to lack of IT security controls. One material weakness was repeated from the previous year. VA reported 6,304 security incidents of which 10 were reported to FedCIRC and externally to law enforcement. Seventy-two percent of all operational systems integrated security control costs into system life cycle.

Management and Program Performance Highlights Reported by the Department

- As highlighted in the agency report, VA has centralized all incident response capabilities into a single VA Centralized Incident Response Capability, which is the focal point for VA interface with FedCIRC.
- The Department increased the number of systems assessed for risk (76%), and with IT security plans (73%).
- VA has developed several security awareness training tools, and has been working to deploy this training. Some of these tools, as described in the agency report, include web-enabled training, conferences, IT security-related satellite broadcasts, and Cyber Security Practitioner Professionalization Training.

Management and Program Performance Challenges Reported by the Department

- According to the agency, at the date of this report, 39% of VA's systems had been certified and accredited.

Management and Program Performance Challenges Reported by the Inspector General

- As cited in the OIG report, external penetration tests verified that VA systems could be exploited to gain access to sensitive veteran information and benefit systems. As shown in these tests, system control weaknesses could allow complete access and control of key VA health care systems resulting in possible creation of fraudulent prescription orders.
- As stated in the OIG report, VA has not yet developed and complied with specific configuration requirements to adequately meet IT security needs, including the patching of security vulnerabilities.

Responsibility of Agency Program Officials and CIO

Table C.1 of the Department of Veterans Affairs FY2003 FISMA Report															
Principal Office (PO) Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level of risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested**	
		No. Of Systems	% Of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total	**871**	**663**	76%	**632**	73%	**342**	39%	**631**	72%	**633**	73%	**627**	72%	**628**	72%

The Secretary has instituted information security standards for members of the Department's Senior Executive Service to provide greater management accountability for information security, and has centralized the Department's IT program including authority, personnel, and funding under the VA CIO. In addition, the Secretary appointed an agency senior information security officer, who serves as an Associate Deputy Assistant Secretary and heads an office under the CIO to fulfill IT security responsibilities. Overarching mission strategies, as well as structured framework for effective implementation of programmatic goals, are articulated in the VA IT Security Program Management Plan, which is updated quarterly.

Responsibilities of Agency Head

The Department CIO has been empowered with final decision making authority relating to funding IT programs, projects, and initiatives. These actions have reinvigorated the Department's progress toward developing its enterprise architecture and facilitated the inclusion of a security baseline into architecture. The Secretary also established the Review and Inspection Division under the CIO's office, as an independent verification and validation mechanism for ensuring compliance with the Department's security program through on-site inspections and document reviews. Also, a senior agency information security officer has been appointed, who occupies the position of Associate Deputy Assistant Secretary for Cyber and Information Security.