Office of Management and Budget

FY 2002 Report to Congress on Federal Government Information Security Reform

May 16, 2003

TABLE OF CONTENTS

I. Executive Summary

The Federal government has made significant strides in identifying and addressing long-standing information technology (IT) security problems that are both serious and pervasive. As a result of focused efforts over the past year, Federal agencies are demonstrating progress. However, as this report details, much work remains, and while the Administration has applied more rigorous IT security reviews, more threats and vulnerabilities have also materialized.

The purpose of this report is to inform Congress on agency IT security activities and results during FY 2002, as required under the Government Information Security Reform Act (GISRA). GISRA 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. To ensure consistent reporting across agencies, OMB issued guidance that included specific reporting instructions along with quantitative performance measures to more effectively determine agency status and progress. Additionally, the OMB guidance directed agencies to develop plans of action and milestones (POA&Ms) to remediate program and system level IT security weaknesses.

This report is based primarily on agency and IG reports to OMB, along with information provided through POA&Ms and agency IT budget materials. The information and findings in this report are based on work performed during FY 2002.

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. These measures reveal that significant progress was achieved in FY 2002. For example, increases in the percentage of systems with security plans and the percentage of systems certified and accredited. However, much work remains to improve the security of the information and information systems that support the Federal government's missions. Table 2 on page 12 presents a summary of Federal agencies status for their IT security performance from FY 2001 to FY 2002. Table 1 below is an abbreviated government-wide summary:

Table 1. FY 2001 and FY 2002 Government-wide IT Security Performance

Total Number of Systems		Percentage of systems assessed for risk and assigned a level of risk		Percentage of systems that have an up-to-date IT security plan		Percentage of systems authorized for processing following certification and accreditation		Percentage of systems with a contingency plan	
FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
7411	7957	43%	65%	40%	62%	26%	47%	30%	55%

*Data provided from agencies' FY 2002 GISRA reports.

In OMB's FY 2001 GISRA Report to Congress, six common government-wide IT security weaknesses were identified:

- Lack of agency senior management attention to IT security.
- Non-existent IT security performance measures.
- Poor security education and awareness.
- Failure to fully fund and integrate security into capital planning and investment control process.
- Failure to ensure that contractor services are adequately secure.
- Lack of detecting, reporting, and sharing information on vulnerabilities.

A year later, progress is clearly evident across these six areas. While additional efforts are still warranted, the Federal government is heading in the right direction.

Funding for IT security continues to increase and this report examines the impact of spending on IT security. For FY 2002, Federal agencies spent about $2.7 billion from a total IT investment of about $48 billion. OMB estimates FY 2003 funding for IT security of $4.2 billion, and in FY 2004, Federal agencies plan to spend over $4.7 billion on IT security. Based on IT spending data and agency IT security performance, spending more on IT security does not always improve IT security performance. Rather, the key is effectively incorporating IT security in project and agency management actions.

OMB oversees and enforces agency remediation efforts through traditional management and budget processes. These processes enable OMB to hold agencies, including Chief Information Officers and agency program officials, accountable for the security of the information and systems that support their programs. 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 using 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.

Additionally, through agency IT budget materials, agencies are required to incorporate IT security in the development of both new and existing IT investments. 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 corrective action plans; and 4) tie their POA&Ms for an IT investment directly to the business case for that investment.

Finally, the report highlights government-wide milestones for improvement in IT security that OMB identified and included in the President's FY 2004 budget. These milestones address key government-wide weaknesses.

- All agencies must establish and maintain an agency-wide process for developing and implementing program and system level plans. POA&Ms must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses are remediated. **The FY 2004 President's Budget established the goal that**

by the end of 2003, all agencies shall create a process that ensures 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.

- Many agencies find themselves faced with the same security weaknesses year after year, e.g., systems that lack security plans and have not been certified and accredited. OMB will continue to assist agencies in prioritizing and reallocating funds to address these problems. **The FY 2004 President's Budget established the goal that by the end of 2003, 80 percent of Federal IT systems shall be certified and accredited.**

- While agencies have made improvements in integrating security into new IT investments, significant problems remain, particularly in ensuring security of legacy systems. **The FY 2004 President's Budget established the goal that by the end of 2003, 80 percent of the Federal government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment.**

Appendix A is a summary of the Federal government's IT security program, highlighting the roles and responsibilities of agencies. Appendix B provides a brief summary of small and independent agencies that submitted a report. 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.

II. Introduction

A. Purpose and Scope of Annual IT Security Report

The Government Information Security Reform Act (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). Additionally, GISRA codified existing OMB IT security policies found in OMB Circular A-130 on IT management and OMB budget guidance in Circular A-11. As a result, GISRA both integrated and reinforced long-standing IT security requirements. GISRA also introduced new review and reporting requirements. Agency Chief Information Officers (CIOs) and program officials are responsible for conducting annual IT security reviews of their programs and the systems that support their programs. Additionally, agency Inspectors General (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.

It is important to note the key principles GISRA emphasized. First, all agency IT security programs and practices must be incorporated into an agency's overall program as well as capital planning process and other management and budget processes. Second, IT security is the responsibility of every Federal employee. 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. Third, by dividing IT security programs into three basic components – management, implementation, and evaluation – GISRA recognized that while security has a technical component, it is at its core an essential management function.

This report serves as both a summary of agency efforts and OMB actions in FY 2002 and provides direction for further improving IT security performance in FY 2003. The agency summaries in Appendix C are based solely on agency and IG work conducted in FY 2002 and do not include any efforts undertaken after September 2002. However, it is important to note that since completion of their FY 2002 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.

B. Continuation of IT Security Efforts Under the Federal Information Security Management Act

GISRA's annual review and reporting provisions expired in November 2002. To ensure the continuation of these important requirements along with the ability to effectively monitor progress, the Congress passed and the President signed into law the Electronic Government Act of 2002. Title III of that Act, the Federal Information Security Management Act (FISMA), permanently reauthorized the framework laid out in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems through the development of minimum standards for agency systems. The National Institute of Standards and Technology (NIST) will work with agencies in the

development of those standards per their statutory role in providing technical guidance to Federal agencies.

III. OMB IT Security Guidance

A. Reporting Instructions and Measuring Performance

In July 2002, OMB provided instructions for Federal agencies' reporting the results of their annual reviews and evaluations. Agencies' FY 2001 reports established a baseline of agency IT security status. To ensure that progress could be consistently determined against that baseline, the FY 2002 reporting instructions remained nearly identical to the FY 2001, which had been closely aligned with the requirements listed in GISRA. Additionally, as part of the FY 2002 guidance, OMB, working with the agencies, took steps to provide the Congress with additional information from agency POA&Ms to ensure appropriate oversight. As a result, the combination of the GISRA reporting requirements, OMB's reporting instructions, and information from agency POA&Ms have resulted in a substantial improvement of the accuracy and depth of information provided to Congress relating to IT security.

Government-wide IT Security Assessment Tool

The development of an automated assessment tool for agency FY 2002 reviews played an important role in guiding and increasing the number of systems reviewed. In 2001, NIST developed a security questionnaire, which greatly assisted agencies in performing self-assessments of their IT systems. This questionnaire was based primarily on NIST technical guidance and the General Accounting Office's (GAO) Federal Information System Controls Audit Manual and allows agencies to assess the management, operational, and technical controls of their systems. Agencies were directed through OMB guidance to use this document as the basis for conducting their annual reviews under GISRA. Under NIST's leadership, this questionnaire was automated in 2002. Agencies have a free automated tool to assist them in conducting their annual reviews. The tool facilitates IT security reviews while improving the quality of the overall process. This tool is available at http://csrc.nist.gov/asset/.

IT Security Performance Measures

One of the most significant additions to the FY 2002 OMB reporting guidance was the introduction of government-wide IT security performance measures. Consistent with GAO's findings, measures were incorporated within the existing instructions, requiring agencies and IGs to report the results of their reviews against the measures. Through these performance measures, the Federal government has a clear picture for the first time of IT security status and progress. For example, agencies were required to report of their total number of systems in FY 2001 and FY 2002, how many had system security plans and how many had been certified and accredited in FY 2001 and FY 2002. From agency responses, areas of progress as well as areas of problems were evident. A table of agency performance against the IT security measures can be found on page 12.

B. Plans of Action and Milestones

OMB guidance also directs Federal agencies to 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 guidance to agencies for reporting under FISMA directs agency IGs to verify whether or not an agency has a process in place that meets criteria laid out in OMB guidance. OMB has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard. An IG verified agency-wide POA&M process is one of three criteria necessary for agencies to improve their IT security status on the Expanding E-Government Scorecard.

C. Budgeting for IT Security

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, i.e., development of security plans and certification and accreditation. Failure to appropriately incorporate security in new and existing IT investment automatically requires the business case to be scored as "at-risk". As a result, that system is not approved to proceed for the fiscal year in which the funds were requested until the security weaknesses are addressed. As of the submission of this report, there are approximately 500 systems in the FY 2004 budget, totaling nearly $18 billion, at-risk either solely or in part due to IT security weaknesses. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems have an out-of-date certification and accreditation.

Spending on IT security continues to increase. For FY 2002, Federal agencies spent about $2.7 billion from a total IT investment of about $48 billion. OMB estimates FY 2003 funding for IT security of $4.2 billion, and in FY 2004, Federal agencies plan to spend over $4.7 billion on IT security. Based on IT spending data and agency IT security performance, spending more on IT security does not always improve IT security performance. An analysis of IT security spending and security results demonstrates 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 early in the life of IT systems.

IV. OMB's Government-wide Findings

A. Progress from FY 2001

Six Common Government-wide IT Security Weaknesses From FY 2001

In the FY 2001 summary report to Congress, OMB identified six common government-wide weaknesses based on our review of agency and IG reports. A year later, progress is clearly evident across these six areas and while additional efforts are still warranted, the Federal government is heading in the right direction.

1. *Increasing agency senior management attention to IT security*. At the end of each fiscal year, agency heads now submit the results of their IT security reviews to OMB. Based on that work, along with agency remediation efforts, and IT budget materials, OMB annually either conditionally approves or disapproves agency security programs. The conditional approval or disapproval of agency IT security programs is directly communicated between the OMB Director and each agency head. In addition, OMB used the President's Management Agenda Scorecard to focus attention on serious IT security weaknesses. Through the scorecard, OMB and senior agency officials monitor agency progress on a quarterly basis. As a result, senior executives at most agencies are paying greater attention to IT security.

2. *Development of IT security performance measures*. As discussed earlier in this report, the absence of government-wide IT security performance measures was addressed in FY 2002 in the OMB reporting instructions. These high-level management performance measures assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific IT security requirements. Agencies reported the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. These measures are mandatory and help to ensure that accountability follows authority.

3. *Improving security education and awareness*. Through the Administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were available to all Federal agencies in late 2002. Initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers, and the general workforce. Additionally, agencies have held IT and information security training sessions for their workforces.

4. *Increasing integration of security into capital planning and investment control*. OMB continues to aggressively address this issue through the budget process, to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Through this process agencies can demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. OMB also provided agencies guidance in determining IT security costs of their IT investments. As a result, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved IT security performance.

Additionally, agencies have made improvements in integrating security into new IT investments. However, significant problems remain in regards to ensuring security of legacy systems.

5. *Working toward ensuring that contractor services are adequately secure*. Through the Administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board, an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. This issue is currently under review by the Federal Acquisition Regulatory Council to develop, for government-wide use, a clause to ensure security is appropriately addressed in contracts.

6. *Improving process of detecting, reporting, and sharing information on vulnerabilities.* Early warning for the entire Federal community starts first with detection by individual agencies and reporting to incident response centers at the Department of Homeland Security (DHS), the FBI, the Department of Defense, or elsewhere. While it is critical that agencies and their components report all incidents in a timely manner it is also essential that agencies actively install corrective patches for known vulnerabilities. To further assist agencies in doing so, the Federal Computer Incident Response Center (FedCIRC) awarded a contract on patch management. Through this work FedCIRC is able to disseminate patches to all agencies more effectively. In addition, OMB and the CIO Council have developed and deployed a process to rapidly identify and respond to cyber threats and critical vulnerabilities. As FedCIRC and related organizations have moved to DHS, additional progress is being made on sharing information needed for Federal agencies to respond to vulnerabilities and cyber threats.

IT Security and E-Government Initiatives

OMB's work on Expanding E-Government under the President's Management Agenda identifies IT security as a key issue. Two of the initiatives, E-Training and E-Authentication provide significant opportunities for leveraging the Federal government's resources to improve IT security. The benefits of the E-Training initiative were identified above. Through the E-Authentication e-government initiative, the Administration deployed and tested a prototype e-Authentication capability in September. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls across government. The full capability is expected in September 2003.

B. New Challenges Identified in FY 2002

The FY 2002 GISRA reports identify a number of positive outcomes: 1) more Departments are exercising greater oversight over their bureaus; 2) at many agencies, program officials, CIOs, and IGs are engaged and working together; 3) IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process; 4) more agencies are using their POA&Ms as authoritative management tools to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected; and 5) OMB conditional approval or disapproval of agency IT security programs resulted in senior executives at most agencies paying greater attention to IT security at their agencies.

At the same time it follows that the more reviews conducted, the more weaknesses agencies find. Therefore, agency reports also identify some troubling government-wide issues and trends:

1) Many agencies find themselves faced with the same security weaknesses year after year, such as a lack of system level security plans and certifications and accreditations. Through the budget process, OMB will assist agencies in prioritizing and reallocating funds to address these problems;

2) Some IGs and CIOs have vastly different views of the state of the agency's security programs. OMB will highlight such discrepancies to agency heads;

3) Many agencies are not adequately prioritizing their IT investments and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process;

4) GISRA requires that agencies review all programs and systems every year. Based on the information in the reports, not all agencies are successfully reviewing all programs and systems each year; and

5) While 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. This particular issue requires the Federal government to think of security in a new manner. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments.

All Federal employees must recognize and fully meet their security responsibilities in order to appropriately secure our government's operations and assets. Those agency officials with additional responsibilities, such as agency program officials and the agency CIO must be held accountable for meeting those responsibilities. The owner of a system must work with their agency CIO to ensure that security has been incorporated throughout the entire life-cycle of a system, from planning and development through operations and maintenance. Increased understanding of IT security requirements along with improved accountability will assist program officials in successfully securing their programs and services. OMB will continue to reinforce the responsibilities of agency program officials and CIOs via management and budget processes.

IT Security Performance Measures

Table 2 provides a summary of Federal agencies' performance against IT security measures. This table identifies both clear progress from FY 2001 to FY 2002 and reveals areas of weaknesses.

Table 2. FY 2001 and FY 2002 IT Security Status and Progress by Agency

Agency	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 authorized for processing following certification and accreditation		Number of systems that are operating without written authorization		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	
	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
Agency for International Development	89	89	28	85	12	63	10	89	79	0	5	20	15	75	13	38	1	3
Agriculture	580	605	59	111	325	142	42	46	538	559	146	156	105	125	136	143	65	62
Commerce	646	609	475	571	447	584	311	467	335	142	542	520	438	521	347	493	61	83
Defense	155	155	125	106	130	103	95	85	60	70	48	62	35	43	131	103	33	32
Education	57	92	42	92	22	36	0	0	57	92	0	0	38	49	32	40	14	37
Energy	961	906	587	597	719	720	205	420	756	486	468	488	532	554	203	221	130	148
Environmental Protection Agency	189	168	174	168	168	156	172	146	17	22		129	87	107		94		31
Federal Emergency Management Agency	51	51	0	8	13	13	0	0	51	51	0	5	0	8	5	8	0	0
General Services Administration	42	56		20	26	29	6	7	36	49	39	22	1	7		21		12
Health and Human Services	277	283	21	122	38	107	10	31	267	252	136	230	45	95	40	93	15	44
Housing and Urban Development	48	127	42	119	46	107	41	92	7	35	44	99	41	97	48	127	48	127
Interior	224	224	27	42	34	70	18	49	206	175	65	109	26	51	36	63	17	23
Justice	235	275	194	210	157	196	194	209	41	66	118	148	128	143	91	117	18	29
Labor	52	46	49	45	49	44	15	32	37	14	42	41	38	42	47	46	14	14
National Aeronautics and Space Administration	1,694	1,641	183	1,641	183	1,489	183	1,459	1,511	182	183	1,641	183	1,600	162	1,600	152	1,453
National Science Foundation	15	20	12	20	10	18	0	6	15	14	15	20	6	20	6	11	6	9
Nuclear Regulatory Commission	23	18	2	18	2	18	2	9	21	9	15	18	2	10	2	13	0	7
Office of Personnel Management		42		5		4		0		42		0		9		6		6
Small Business Administration	37	37	14	22	15	22	14	24	23	13	0	5	0	2	7	7	7	7
Social Security Administration	16	17	16	17	16	17	16	17	0	0	16	17	16	17	16	17	15	16
State		344		256		53		0		344		30		189		38		0
Transportation	427	677	220	85	113	97	111	56	316	621	102	110	146	100	119	114	43	49
Treasury	598	624	343	258	131	261	101	266	497	358	355	486	302	418	233	326	53	77
Veterans Affairs	995	851	582	542	330	581	407	262	588	589	662	563	263	469	547	603	536	499
TOTAL	**7411**	**7957**	**3195**	**5160**	**2986**	**4930**	**1953**	**3772**	**5458**	**4185**	**3001**	**4919**	**2447**	**4751**	**2221**	**4342**	**1228**	**2768**
TOTAL Percentage			**43%**	**65%**	**40%**	**62%**	**26%**	**47%**	**74%**	**53%**	**40%**	**62%**	**33%**	**60%**	**30%**	**55%**	**17%**	**35%**

V. Process to Improve Performance

Building from the framework in GISRA, a roadmap to continue to improve IT security performance has been identified and reinforced through existing management and budget processes. Listed below are five areas in which OMB will continue to work with agencies to ensure that the Federal government further advances its progress to safeguard our information and systems.

A. Plan of Action and Milestones Process

To ensure that remediation plans continue to be developed, implemented, and corrective actions prioritized and tracked, each agency must put in place a robust agency-wide plan of action and milestone process. As part of IG's FY 2003 FISMA work, OMB guidance will instruct IGs to assess whether such a process exists. A robust process, verified by agency IGs is one of three criteria agencies must meet to "get to green" for security on the Expanding E-Government Scorecard.

B. IT Security Performance Measures

To assist agencies and OMB in better tracking progress, agencies will begin reporting on a quarterly basis with their POA&M updates, their status against the IT security performance measures in OMB guidance. These updates will help inform the quarterly assessment of the President's Management Agenda Scorecard.

C. President's Management Agenda Scorecard

Outside of OMB's annual conditional approval or disapproval of agency 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.

D. Government-wide Milestones for IT Security

OMB set targeted milestones for improvement for some of the critical IT security weaknesses in the President's FY 2004 budget. Targets for improvement include:

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

- Many agencies find themselves faced with the same security weaknesses year after year, such as a lack of system level security plans and certifications and accreditations. Through the budget process, OMB will continue to assist agencies in prioritizing and reallocating funds to

address these problems. By the end of 2003, 80 percent of Federal IT systems shall be certified and accredited.

- While agencies have made improvements in integrating security into new IT investments, significant problems remain in ensuring security of legacy systems. By the end of 2003, 80 percent of the Federal Government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment.

E. Threat and Vulnerability Response Process

Experts agree that it is virtually impossible to ensure perfect security of IT systems. Therefore in addition to constant vigilance on IT security we require agencies to maintain business continuity plans. In FY 2002, OMB directed all large agencies to undertake a Project Matrix review to ensure appropriate continuity of operations planning in case of an event that would impact IT infrastructure. Project Matrix was initially developed by the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector. The CIAO and its functions were transferred to DHS on March 1, 2003.

Coordination of the Federal government's cyber security and critical infrastructure protection efforts continues under the leadership of the new Homeland Security Council's (HSC) Special Assistant to the President for Critical Infrastructure Protection, and the Assistant Secretary for Infrastructure Protection at DHS, in partnership with OMB. OMB works with the HSC and DHS, and all Federal agencies to ensure that through IT security policy and management and budget processes, our critical operations and assets are appropriately identified along with the resources necessary to secure them. We are also working with DHS to improve the Federal government's response to cyber attacks and vulnerabilities. The integration of 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, partnering with the Science and Technology directorate on research and development needs, presents an opportunity for the Administration to strengthen government-wide processes for intrusion detection and response and improve critical infrastructure protection through maximizing and leveraging the important resources of these previously separate offices.

VI. Conclusion

GISRA has clearly been instrumental in improving the state of Federal IT security. The framework and processes in law and OMB policy have reinforced the importance of management, implementation, evaluation, and remediation to achieving real IT security progress. Due to the significant work of Federal agencies and IGs, we are able to point to real advancement in closing the Federal government's IT security performance gaps. That said, many pervasive IT security weaknesses remain, leaving the Federal government with significant risks. OMB will continue to work with agencies, Congress, and GAO to ensure that appropriate risk-based and cost-effective IT security programs, policies, and procedures are in place to secure our operations and assets, ultimately 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.

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 guidelines 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 NIST issues

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

technical guidance (via Federal Information Processing Standards and Special Publications). 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 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.

National Institute of Standards and Technology. NIST, under the Department of Commerce (DOC), is responsible for developing technical security standards and guidelines for sensitive but unclassified Federal information and systems under the Computer Security Act. Again, the PRA, Clinger-Cohen Act and FISMA all reinforce NIST's role. OMB policy requires that agency security programs and practices be consistent with NIST guidance. NIST performs their statutory responsibilities through their Computer Security Division.

2. Assistance, Advice and Operations:

Department of Homeland Security. The following previously separate offices and their functions were transferred earlier this year to the new Department of Homeland Security (DHS) under DHS' Information Analysis and Infrastructure Protection (IAIP) Directorate. Specifically, 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 serves 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.

The integration of these offices and their functions under the IAIP Directorate of DHS, presents an opportunity to both strengthen government-wide processes for intrusion detection and response and improve critical infrastructure protection through maximizing and leveraging the resources of these previously separate offices.

Appendix B: Reporting by Small and Independent Agencies

Background

OMB intensified efforts in FY 2002 to improve participation by the small and independent agencies in the GISRA process. As a result of joint efforts with the Small and Independent Agency CIO Council, 58 agencies submitted GISRA reports, an increase of 24 over FY 2001.

Of the 58 agencies that submitted reports, 27 did not include an independent assessment that met GISRA requirements. 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 IT security program.

The small and independent agencies budgeted over $47M for IT security in FY 2002, predominantly for personnel costs and equipment. This figure is conservative, given that one quarter of the small agencies did not track the amount of money spent to protect their information and information systems.

Twenty-six agencies subject to GISRA did not submit reports in FY 2002. The majority of these agencies have less than 100 full time employees.

Agencies with identified Material Weaknesses

A crosscut analysis of GISRA reports shows that 21 agencies 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. There was a lack of standardization amongst the agencies in terms of what was reported as a significant deficiency. Some agencies that should have reported a material weakness in their IT security policy, procedure or practice, did not.

The overall number of material weaknesses at the small and independent agencies decreased from 303 in FY 2001 to 128 in FY 2002. The decrease in material weaknesses is partially attributable to agencies aggregating numerous, detailed weaknesses into fewer broad categories.

Forty-eight material weaknesses are repeated from FY 2001.

Identification of Mission Critical Systems

GISRA 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.

Thirty-nine small and independent agencies documented their critical operations and assets. Ten others are in the process of determining the importance of specific architectural components.

Contracts with Larger Agencies for IT services

Many small and independent agencies outsource portions of their IT system management to one of the 24 CFO Act agencies. The large agencies that most commonly provide support are:

- Department of Interior's National Business Center for financial management, accounting, procurements and contracts
- Department of Agriculture's National Finance Center for payroll, personnel, administrative payments, accounts receivable, property management, budget and accounting activities
- Department of Treasury's Bureau of Public Debt for payroll and personnel services as well as maintenance of software and data and security services.
- Department of the Treasury's Electronic Certification System (ECS) for payments.
- General Service Administration for payroll, human services and financial management
- Department of Transportation's Federal Financial Management System

Risk Management Programs at the Small and Independent Agencies

a. Risk Assessment
Twenty-three of the small and independent agencies assessed each of their systems for risk. The remaining agencies are equally divided between those that conducted risk assessments for a subset of their systems and those that conducted no risk assessments at all.

b. Security Plans
Fifteen agencies developed security plans to document the management, technical and operational controls designed to reduce risk for each of their systems. Ten agencies prepared plans for a portion of their systems. Twenty agencies have no written security plans.

c. Certification and Accreditation
Eight agencies certified and accredited all of their systems to operate within specific risk parameters. Management officials at these agencies 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 29 agencies not conducting any certification or accreditation activities.

Maturity of Technical Controls

a. Patch management
The majority of small agencies reported that they monitor vendor as well as government websites for updates on patch availability. In general, agencies tested patches before uploading them to the network. Both manual and automated processes are used to distribute patches.

Seven agencies did not provide information on their patch management processes. Three agencies admitted they did not have formal, written procedures for tracking installation of patches.

b. Testing of Agency Security Controls

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

Twenty-nine agencies reported that they tested security controls for less than 50% of their systems. Eight agencies did not test security controls at all.

On a positive note, the percentage of systems being tested rose for 24 agencies in FY 2002.

Incident Handling Programs

In accordance with GISRA requirements, agencies must institute procedures for detecting, reporting, and responding to security incidents. Civilian agencies are required to report IT security incidents to FedCIRC.

Although 4 agencies maintained comprehensive logs containing over 5000 incidents, other agencies reflected a lack of maturity in their incident handling programs.

Two agencies reported that they did not have an incident reporting function. Twelve agencies asserted that they had an incident handling capability but had not had any incidents for the entire year. Ten agencies had security incidents but did not report them to FedCIRC.

Incident reporting is not at an acceptable level for the small and independent agencies. One agency IG stated that "the lack of internal procedures for incident reporting undermine the effectiveness of any external reporting to FedCIRC."

OMB will work with FedCIRC to determine root causes for the performance gaps in agency incident detection, handling and reporting programs.

Security Awareness, Training and Education

a. For Agency Employees Including Contractors

Agencies reported several types of security training for employees, including orientation, annual refresher training and specialized training (i.e., for users of laptops). Training methods included self study CDs, videos, websites with automated tracking systems, and personal instruction.

Nine agencies reported that they provided annual security training for 100% of their staff. At the other end of the scale, 13 trained less than 10% of their personnel.

With the exception of six agencies that did not record the number of employees trained, the remaining agencies reported that their security education, training and awareness programs reached a moderate number of their workforce.

b. For Employees with Significant Security Responsibilities

The agencies reported that of 1052 employees with significant security responsibilities, 387 received training in FY 2002. Of the 37% who received training, specialized instruction was provided in practices such as firewall maintenance, auditing, and contingency planning.

Training methods included government and vendor seminars as well as software development sessions.

Three agencies did not record training for system administrators.

Continuity of Operations

a. Plan Preparation
Although 17 agencies developed continuity of operations plans for all of their IT systems, 9 agencies had done no contingency planning. The remaining agencies had prepared plans for selected systems, most often for 50% or less of their IT infrastructure.

b. Testing
Contingency plans that are periodically tested are more viable than those that are not. Five of the agencies serve as role models in this regard, and completed contingency tests of 100% of their systems.

Testing of contingency plans remains a concern, however, with only 18 agencies conducting any testing at all.

Remediation of Identified Security Weaknesses at Small and Independent Agencies
In FY 2001, thirty-five agencies submitted reports detailing the status of agency IT security programs. Thirty-three of these agencies subsequently developed plans of action and milestones to implement appropriate remedial actions.

Collectively, the agencies identified a total of 797 weaknesses. Of this number, roughly half (396) were reported corrected by the agencies at the end of FY 2002.

Reasons for non completion of milestones included an inaccurate estimate of the resources needed to complete the job, a change in management, or a shift in management priorities.

OMB will continue to track open action items using the quarterly security updates from the agencies.

Conclusions
Although many of the small and independent agencies made measurable progress in identifying and correcting security vulnerabilities, an increased level of effort is required in order to ensure compliance with GISRA requirements. In particular, small and independent agencies must document the sensitivity and criticality of all IT systems, identify risks, and undertake follow on activities to bring risks to an acceptable level.

OMB will closely monitor progress by the small and independent agencies in implementing cost effective security controls.

Small and independent agencies that submitted GISRA reports:

Access Board*
American Battle Monuments Commission
Appalachian Regional Commission
Barry Goldwater Scholarship and Excellence in Education Foundation*
Broadcasting Board of Governors
Christopher Columbus Fellowship Foundation*
Corporation for National and Community Service
Court Services and Offender Supervision Agency
Defense Nuclear Facilities Safety Board
Executive Office of the President, Office of Administration
Executive Office of the President, the United States Trade Rep
Export/Import Bank of the United States
Farm Credit Administration
Federal Communications Commission
Federal Deposit Insurance Corporation
Federal Energy Regulatory Commission
Federal Housing Finance Board
Federal Labor Relations Authority
Federal Maritime Commission
Federal Reserve System
Federal Trade Commission
Inter-American Foundation*
Institute of Museum and Library Services
Japan-US Friendship Commission*
James Madison Memorial Fellowship Foundation*
Marine Mammal Commission*
Morris K. Udall Foundation
National Archives and Records Administration
National Capital Planning Commission*
National Credit Union Administration
National Endowment for the Arts
National Endowment for the Humanities
National Gallery of Art
National Labor Relations Board
National Mediation Board
National Transportation Safety Board (included with DOT submission)
Nuclear Waste Transportation Safety Board
Occupational Safety and Health Review Commission
Office of Special Counsel
Overseas Private Investment Corporation
Peace Corps
Pension Benefit Guaranty Corporation
Postal Rate Commission
Railroad Retirement Board
Securities and Exchange Commission
Selective Service

Smithsonian Institution
Tennessee Valley Authority
The Committee for Purchase from People who are Blind or Severely Disabled
U.S. Chemical Safety and Hazard Investigation Board
U.S. Commodity Futures Trading Commission
U.S. Consumer Product Safety Commission
U.S. Equal Employment Opportunity Commission
U.S. Holocaust Memorial Council
U.S. International Trade Commission
U.S. Merit Systems Protection Board
U.S. Trade and Development Agency*
U.S. Office of Government Ethics

Additionally, in November 2002, OMB requested that microagencies (agencies highlighted above with an *) that had not yet submitted a GISRA report, provide answers to the following questions:

1. Name of all general support systems and major applications
2. Name of person responsible for the system or application (If application is owned or managed by another agency, please provide that agency's name.)
3. Purpose of the system or application
4. Sensitivity of the information stored within, processed by, or transmitted by the system/application, i.e. high, medium or low
5. Criticality of the system/application, i.e. high, medium or low
6. Existence of a security plan for the system/application (yes, no)

Agency responses are an incremental step in the planning and implementation of security measures for microagency IT systems.

Appendix C: Individual Agency Summaries for the 24 CFO Act Agencies

Department of Agriculture (USDA)

A. General Overview

1. Security funding.
The Department of Agriculture reports planned FY 2003 funding for IT security of $64M. This funding level comprises 3% of their total planned IT portfolio of $2.13B.

2. Number of programs reviewed.
The IG and Department reported different numbers for the total number of programs and systems and the total number reviewed in FY 2002. Of a total of 25 programs the IG reported that the Department reviewed 9 of them in FY 2002; of a total number of 349 systems the IG reported that the Department reviewed 152 of them in FY 2002.

In FY 2002, USDA reported a total of 18 programs, all of which they stated were reviewed. The Department reported a total of 605 systems, of which 150 were reviewed.

3. Material weaknesses.
The IG reported a total of 70 material weaknesses in FY 2002, with 14 of them being repeated material weaknesses from FY 2001. The IG noted that the Department did not have security plans in place for all its major applications and general support systems, had not planned for contingencies, and had not certified security controls in place and authorized processing for all of its systems. Nor had the Department identified all of its mission-essential infrastructure, conducted risk assessments, or prepared mitigation plans on the identified risks.

USDA reported seven security functional areas as material weaknesses in FY 2001. These weaknesses were described in categorical terms rather than at the agency or system level, as all agencies were deficient in some regard. The material weaknesses reported by the Department were in the areas of physical security, access controls, intrusion detection, risk management, configuration management, system certification, and contingency planning. In FY 2002, the Department reported 197 material weaknesses, with 66 repeated from FY 2001. These material weaknesses were compiled from agency self-assessments conducted for the FY 2002 GISRA report. However, USDA's Office of the CIO conducted additional analysis and identified 439 material weaknesses in its security plan review; 201 material weaknesses in its agency self-assessment; and 119 material weaknesses in its on-site review. The Department points out that many of these material weaknesses are duplicates of weaknesses discovered during a previous review, so it is difficult to ascertain correct numbers of material weaknesses, as the Department does not indicate which or how many material weaknesses are repeats of those previously reported.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.

During FY 2002, the Secretary instituted a number of steps, directly and through delegated authority to the CIO, to ensure program and IT executives and managers understand and perform their information security responsibilities. For example, the Department established an information security performance measure within the performance plan of each Under and Assistant Secretary, agency head, and staff office director. Each executive is held accountable for performance on this measure and will be rated on it during the annual performance review. In addition, the Department's Major IT Investment Portfolio is submitted annually for approval by the USDA Executive Information Technology Investment Review Board. Each investment in the Portfolio is evaluated to ensure security is addressed, staffed, budgeted, and assessed for compliance with USDA Cyber Security Policies. Similarly, the CIO reviews each acquisition above a $250,000 threshold to ensure security is addressed, staffed, budgeted and assessed for compliance with Departmental Cyber Security Policies. Security responsibilities and authorities for Program Officials, CIOs, security officers, IT technical specialists and IT users have been established through Departmental guidance and policy.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG reported that the Department cannot be assured that its agencies are adhering to their security plans throughout the life cycle of each system. Historically, USDA's decentralized approach to addressing its agencies' IT security and infrastructure needs has led to a broad array of technical and physical solutions that do not assure that complete Department-wide security is obtained. In FY 2002, the lack of agency management involvement in their respective systems' security planning and implementation continues to be problematic. However, the Department has taken specific steps to oversee the actions of program officials and agency CIO's. The Office of the CIO met with senior program management officials to discuss the deficiencies identified in FY 2001 security plans and worked with them to obtain their commitment to correct these deficiencies.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The Department was working to develop risk assessment checklists that cover the various system platforms used within the Department and made arrangements for agencies to use a contractor to assist them in conducting risk assessments. The Department still needs to finalize its risk assessment policy and follow up with agencies to ensure that they perform and evaluate the assessments. In addition, an effective continuity of operations program cannot be established without first identifying the systems that are critical to meeting the Department's mission. Nor can physical and operational security controls be effectively established without first identifying threats to USDA critical systems and following up with a mitigation plan for those identified risks.

4. Critical asset prioritization and protection methodologies.

USDA did not undergo a Project Matrix review to identify its critical operations and assets, but began discussions with the Critical Infrastructure Assurance Office and will work with

the Office to begin this effort. Until the Project Matrix review is completed, USDA will continue to rely on the analysis it conducted for Y2K to identify mission-critical systems.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG review noted that while suspect intrusion incidents detected at the Department level are being forwarded to agency personnel for follow up, agencies are not always responding to replies or reports of actions taken. The IG reported that the Department did not have an effective methodology for performing follow up on non-responsive agencies and was not able to monitor all agencies' networks requiring monitoring at the agency level. The IG also identified numerous occasions when patches were not installed in a timely manner. USDA indicated that it is planning to implement patch-management in the first quarter of FY 2003.

The Department indicated that it documented a security incident response procedure. However, while notification to agencies is operating effectively at the Department level, additional emphasis is needed in reporting incidents to FedCIRC. USDA reported that incident information is not shared in a timely manner with FedCIRC, with the required average time to report to the agency and FedCIRC following an incident taking up to three days for a preliminary report.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reported that the Department and most of its agencies had not complied with the OMB Circular A-130, Appendix III, and GISRA requirements that agencies assess the risk to their operations and critical IT assets under their control. While the Department provided agencies with checklists to begin assessing the risk to their systems and infrastructure, agencies had not yet incorporated periodic risk assessments in their security programs. In addition, while the Department increased emphasis on preparing security plans through its reviews and corrective action meetings with agency program officials, not all agencies have prepared security plans for all of their major applications. Additionally, the Department and its agencies had not tested and evaluated security controls in place for major applications.

2. Department methods to ensure contractor services are secure.
In conducting agency reviews, the IG limited testing of contractor operations to access controls, security clearances, security awareness training, and oversight by the agencies of contractor activities. Their findings indicated that the Department and its agencies had not ensured that contractor provided services meet the requirements of GISRA, OMB policy, NIST guidelines, and agency policy.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG was unable to obtain performance measurement information on security training. While IG reviews identified a lack of security awareness training in many of the agencies

tested, specific numbers of employees who have received this training was not identified. Agencies were not able to provide a listing of agency contractors and as a result, the IG was unable to determine the total number of employees and contractors.

USDA indicated that the CIO began planning a USDA Cyber Security Awareness and Training Program. The CIO conducted agency interviews to establish a current cyber security awareness baseline. In addition, the CIO will select a contractor to support the selection of commercial security training tools for USDA executives, develop a long-term awareness strategy, identify commercial products and services to fulfill USDA security training needs, and define a methodology for measuring the effectiveness of USDA's security awareness and training program.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
The Department had not fully integrated security into the capital planning and investment control (CPIC) process for FY 2003. Agencies had not reported all the security requirements and costs on all FY 2003 capital asset plans or OMB Exhibit 53 submissions reviewed by IG. While budget materials for FY 2004 were not available for IG review, the Department updated its CPIC guidance to ensure agencies submit all required security measures and costs in their FY 2004 CPIC documents.

Department of Commerce (DOC)

A. General Overview

1. Security funding.
The Department reports planned FY 2003 funding of $64M for IT security and critical infrastructure protection for its fourteen agency components (operating units), which includes the U.S. Patent and Trademark Office. This funding level comprises 4.7% of their total planned IT portfolio of $1.36B.

2. Number of programs reviewed.
The Department reported that it reviewed 512 systems of the total 646 systems in its fourteen agency components in FY 2001. In FY 2002, 604 of the total 609 systems were reviewed. Of the 37 total agency programs, 33 were reviewed in FY 2002.

The Department used the NIST system self-assessment guide for the review of systems and programs in FY 2002.

3. Material weaknesses.
The IG noted that the Department should continue to report information security as a material weakness until all of the Department's national-critical and mission-critical systems are

accredited. While significant strides were made in the establishment of a foundation for an effective information security program, the IG stated that there was more room for improvement, given the severity of the Department's information security weaknesses.

As a performance-based organization, USPTO conducted its own information security review and submitted its FY 2002 GISRA report separately from the Department along with the IG's independent GISRA review. The IG reported that USPTO lacks up-to-date security plans and current accreditations for its operational systems and should consider information security a material weakness, which USPTO declared for FY 2002. The IG recommended that information security continue as a material weakness until all mission-critical systems have been accredited.

As of the date of the September report, the Secretary had not yet determined the Department's material weaknesses for FY 2002. While the FY 2001 report referenced the Department's implementation of IT management controls to improve IT security, the Office of the Chief Information Officer recommended that IT security be repeated as a material weakness.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.

The Department issued a memorandum advising program officials of their IT security responsibilities. Program officials are required to provide adequate resources, including funding, to ensure the security of the Department's IT assets. Performance plans for all CIOs are now inclusive of IT management accountability. An IT Review Board was established by the Department with the Department CIO as chairman. The Board reviews proposals of new initiatives and requests for major IT acquisitions, as well as performs control and evaluation reviews of ongoing IT projects.

The Department reallocated staff to support IT security program functions. Six full-time IT security staff were reassigned to assist the four existing staff members. Additional FY 2001 funding was made available to let an IT security contract for IT security activities in FY 2002. The contract provided support in IT security compliance reviews and for additional staffing of the Department's Computer Incident Response Team (CIRT).

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG's review indicated that a number of operational systems had not been certified and accredited and those that were lack evidence that security testing and evaluations had been performed. The IG indicated that improving information security remains a priority and that the Department should focus on system security plans to assure adequate content and quality and also comply with the certification and accreditation process.

The Department's IT security policy requires the consideration of IT security in all phases of the system life cycle. The Department indicated that the focus for FY 2003 is to improve Department-wide certification and accreditation practices.

The Secretary, through the Office of the CIO, established a strong IT security program. There is a direct link between the IT Security Officer (ITSO) for the Office of the Secretary (O/S) and the IT Security Program Manager to ensure that the ITSO is adequately trained and carries out the ITSO duties, which include ensuring that the O/S's information security plan is practiced throughout the life cycle of each system. The Department took specific actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The IG reported that systems considered to have national critical importance have priority in reviews performed by the Office of the CIO. The FY 2001 report indicated that the Department was making an effort to improve information security and required that it be an integral component of the Department business operation. In this effort, the Department established a Critical Infrastructure Program (CIP) team and appointed an IT Critical Infrastructure Program Manager. Additionally, the Secretary directed officers and heads of operating units to 1) give information security high priority, sufficient resources, and their personal attention, and 2) restructure and strengthen IT management by requiring a unit CIO to report to the unit head or principal deputy and to the Department CIO.

4. Critical asset prioritization and protection methodologies.

The IG reported in FY 2001 that the reliability of the Department's asset inventory for the CIP program was questionable because of weaknesses in the methodology used to gather asset data. The IG maintained concern in this critical area for FY 2002. The IG's concern stems from the fact that the Department did not begin assessing Project Matrix until March 2002, and is not expected to have a draft report detailing the results until October, 2002. No timeframe for completion on the second phase - public sector dependency analysis - was provided by the Department.

The Department initiation of Phase 1 of the Project Matrix review has resulted in identification of 42 mission critical assets, of which approximately 10 may be considered nationally critical. These assets receive highest priority in the allocation of Commerce IT security resources. The Department advised that it was in the process of identifying asset interdependencies and assessing risk.

5. Department documented procedures for reporting and sharing vulnerabilities.

The FY 2001 IG report indicated that the Department had four agency components with formal incident response capability. For FY 2002, the Department reported that all 14 agency components maintain an incident handling and response capability. Five of the agency components with formal Computer Incident Response Teams (CIRTs) report to FedCIRC within 24 hours of the incident discovery. The IG FY 2002 report echoes that of

the Department. In FY 2002, the Department reported these five CIRTs were established to support the Department's operating units. NIST, NOAA, Census, and the USPTO have their individual CIRT and the remaining bureaus' rely on the Department CIRT for assistance. Advisory information is provided to the system security officers by way of the Department CIRT, FedCIRC, and the NIPC. The Department is in the process of upgrading its incident detection capability, intrusion detection, incident response and reporting capabilities, and providing improved event monitoring. The Department reported 149,703 incidents for FY 2002 with 36,507 of these incidents referred to FedCIRC or law enforcement.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
As of July 2002, at the conclusion of its fieldwork, the IG reported a pervasive lack of risk assessments among the operating units, as well as numerous systems operating without approved security plans or accreditation. In addition, the IG found documentation of security control testing for only one system.

In FY 2001, the Department reported two important steps toward achieving the goal of improved information security and including the improved IT security as an integral component of the Department's business operations. These steps included the directive of the Secretary to Secretarial officers and heads of operating units to 1) give information security high priority, sufficient resources, and their personal attention and 2) restructure, and thus strengthen, IT management by having a CIO at each unit who reports to the unit head or principal deputy and to the Department CIO. The Department reported that 95% of the Department's systems have been assessed for risk, a 25% increase over FY 2001. Seventy-eight percent of the operating systems have been authorized for processing following certification and accreditation. This represents a 29% increase over FY 2001, with 22% of the systems vulnerable to security risks remaining. Contingency plans are in effect for 493 systems, which constitutes 82% of the total systems. However, only 17% of these plans were tested in the past year. Although there has been an overall improvement in the IT security performance over last year, there is still room for significant improvement.

2. Department methods to ensure contractor services are secure.
The IG reviewed 40 of the Department's IT service contracts and found that there were insufficient or nonexistent safeguards for sensitive but unclassified systems and information. The IG evidenced concern in this area as a "lack of sufficient policy and guidance to ensure that contract documents for IT services contain adequate information security provisions." The IG recommended that the Department take the necessary action to ensure that all contracting offices include adequate information security provisions in all IT service contracts in order to protect the Department's sensitive IT information and assets. Further, the IG recommended that such policy require contracting offices to assess the IT security risk associated with the proposed service or system during the acquisition planning phases; identify and include appropriate information security requirements in specifications and work statements; monitor contractor performance to ensure compliance with information security requirements; and terminate the contractor's access to systems and networks once the

contract is closed out. The Department's FY 2002 report indicated that 9 of the 28 contractor operations or facilities were reviewed in the past fiscal year.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that the Department CIO reallocated staff from lower priority areas to information security and critical infrastructure protection. The Department reported that they implemented a compliance review program and corrective action oversight and tracking process. Although IT security awareness programs were conducted Department-wide, the IG maintained that additional efforts are needed to ensure that employees with significant information security responsibilities receive adequate specialized training and education. Additionally, the IG reported that the operating units need to do a better job of identifying security risks and controls throughout the system life cycle so that security expenditures can be better estimated and justified.

The IG highlighted problems with NIST's information security program and reported that NIST's policy is missing critical control elements, stating that the NIST policy specifically "does not assign responsibilities to the director of NIST and to the CIO for developing, implementing, and maintaining an agency-wide security program." The policy also lacks key controls, including risk management, security control review, life cycle management, certification and accreditation, and contingency planning.

Security training has been a positive aspect of the Department's progress with 100% compliance to employee training, which also includes all contractors. The Secretary emphasized the importance of information security and has clearly stated that "a lack of resources, financial or otherwise, is not an acceptable reason for failure to improve."

2. CIO methods to ensure contractor services are secure.
See item C.2.

3. Agency integration of security and capital planning.

The IG found that most of the capital asset plans specified projected security costs, but only a few plans explained how these funds would be spent. In addition, the IG concluded that the operating units need to do a better job of identifying security risks and controls throughout a system's life cycle so that security expenditures can be better developed and justified. Fifty-two capital asset plans were submitted to OMB during FY 2002. The Department reported that all agency systems were included on their exhibit 53 and all discrepancies have been corrected. The 52 plans were also independently validated prior to submittal to OMB.

Department of Defense (DOD)

A. General Overview

1. Security funding.

The Department of Defense reports planned FY 2003 funding for IT security of their 24 components at $1.943B. This funding level comprises 7% of their total planned IT portfolio of $ 27.7B. This does not include Information Assurance resources embedded in weapons systems nor does it include information security funding related to the Navy Marine Corps Intranet (NMCI).

2. Number of programs reviewed.

In FY 2002, DOD focused its review on networks. Using the Defense Information Services Agency's Connection Approval Process (CAP) database, DOD identified 550 major networks. Of that total population, DOD reported on 366 classified and unclassified networks in its FY 2002 GISRA report. In addition, DOD selected 155 systems for review and assessment from the FY 2001 GISRA sample set of 560 systems. For FY 2002 GISRA requirements, the IG identified the DoD FY 2001 GISRA sample set of 560 systems as its independent subset of systems to review. Specifically, the IG selected and evaluated a statistical sample of 115 collaterally controlled DoD-wide systems from that DoD sample set of 560 systems.

The Department uses the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) enterprise-wide for standardized certification and accreditation (C&A) of its systems, networks, and sites. Many of the basic elements of the NIST guide are contained in the DITSCAP, including the requirement to maintain a system life cycle plan, contingency plan, access controls, and administrative controls.

3. Material weaknesses.

The Department reported that there were eight material weaknesses in FY 2002, one of which is a repeat material weakness from FY 2001. DOD indicated it has undertaken aggressive action to improve and expand its information assurance capabilities to improve upon the following material weaknesses: (1) Complete the implementation of the Information Assurance Vulnerability Alert (IAVA) process to all Services and agencies; (2) Timely distribution of effective computer security policies and procedures; (3) Improve DOD business processes to ensure that all systems are protected. In this area the IG identified six repeat information assurance weaknesses in C&A, security policies and procedures, security training and education, risk assessments, contingency planning, and separation of duties that were identified in the previous information assurance summary reports issued by the GAO, DOD IG, and DOD audit community in 2000 and 2001; (4) Decrease the time necessary for correction of reported weaknesses; (5) Ensure that computer security policies are enforced and security capabilities are tested regularly. The IG identified a material weakness in the effective implementation of DITSCAP. As a result, DOD managers assumed unknown risks to the IT infrastructure, systems, networks, and applications; (6) Ensure that training is conducted for all network personnel (this includes awareness training for all personnel to specific network defense training for system and network administrators); (7) Increase access

security through the use of electronic tokens; and (8) Increase security through certificates (for authentication and repudiation).

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
DOD reported that they have an aggressive IA posture and are constantly striving for improvement. Many of the major tenets contained in the GISRA legislation are already basic elements of DOD's comprehensive information security program. The DOD CIO has established priorities in many of the critical areas identified in GISRA.

The CIO established an Information Assurance Strategy and a complimentary implementation mechanism known as Defense in Depth (DiD). Through a structured and deliberate risk analysis, DiD acts on the premise that a multi-layered approach to the protection of information assets is most effective. The DiD concept is predicated on the use of defense mechanisms on successive layers at multiple locations. To support network-centric performance across the enterprise, DOD is continuing its implementation of DiD. The Department also is implementing a Global Information Grid (GIG), overarching network architecture in development that will facilitate interoperability and the communication and computing needs of the Department.

In addition, the CIO established a number of senior-level bodies that discuss, brief, and shape the future of DOD's IA efforts. These include but are not limited to the DOD CIO Executive Board, and the Military Communications-Electronics Board (MCEB). The CIO Executive Board, chaired by the Department CIO and comprised of CIOs from the Services, DISA, the National Security Agency (NSA) and major elements of the Office of the Secretary of Defense, focuses on advancing the Department's goals in the areas of interoperability, information security, and information management among Defense components. The Board coordinates with the Intelligence Community CIO Executive Council on matters of mutual interest (e.g., integration of the GIG). The MCEB focuses its mission on developing and supporting military communications and electronics matters for the Secretary of Defense, the Joint Chiefs of Staff, and the DOD CIO. It coordinates matters under its jurisdiction among the DOD components, between the DOD and other government agencies, and between DOD and representatives of foreign nations. Proponents of new or changed IT policies or programs often seek the counsel of, and review by, the CIO Executive Board and the MCEB. This enables the boards to develop, enforce, and shape IA policy consistently across the DOD enterprise.

DOD reported that they issued numerous information security policy directives, instructions, manuals, and policy memorandums to address computer security and information assurance. The Department plans to issue new directives and instructions to keep pace with the management challenges that accompany the introduction of new technology and new cyber threats.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
DOD determined that the collection of network metrics would effectively support its emphasis on network-centric operations and enhance its overall IA security reporting. The Department reported that in FY 2002, 352 of the 366 total networks (241 unclassified networks and 125 classified networks) were certified and accredited to operate. DOD reported that 85 of the 155 systems selected in the FY 2002 GISRA sample were authorized for processing following certification and accreditation and 70 were operating without written authorization (including the absence of certification and accreditation).

For FY 2002 GISRA requirements, the IG performed an independent assessment to verify and validate the information security data and status for the sample set of 115 systems that DOD components reported in the DOD FY 2001 GISRA Collection Matrix. To assess the DOD information security posture for GISRA in FY 2001, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD-C3I) identified 28 key information security control measures that DOD components were required to report in the GISRA Collection Matrix. The IG selected and reviewed in detail seven of those information security controls, such as determining whether systems had received C&A (either under DITSCAP or a non-DITSCAP process), functioned under an interim approval to operate, performed risk assessments, developed and implemented contingency plans and system security plans, or whether physical security controls or logical access controls were in place.

The IG found that segments of the DOD GISRA report for FY 2001 on 560 IT systems were not completely valid. This invalid reporting occurred for the sample systems because the DOD components could not substantiate the systems' information security status with adequate supporting documentation, and because the DOD components and ASD-C3I made errors in reporting and summarizing the information security data.

Overall, the results of the Defense audit community's assessment of the DOD FY 2001 GISRA reinforces the position that the ASD-C3I and the DOD components do not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies (including ensuring that the security plan is practiced throughout the life cycle of each system) and ensuring that those policies are consistently practiced throughout the Department.

DOD reported that as a means to ensure the practice of information security throughout a system's life cycle, the Department implemented DOD Instruction 5200.40, DITSCAP. DITSCAP establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit IT systems, networks, and sites. The process certifies that the IT system, network, or site meets the accreditation requirements, and that it will continue to maintain an accredited security posture throughout its life cycle.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The Department assigned DOD Critical Infrastructure Protection (CIP) responsibilities to the Deputy Assistant Secretary of Defense for Security and Information Operations (DASD-S&IO), the senior policy official responsible for the Department's information, physical, personnel, and operational security, as well as information assurance, security, counterintelligence, and information operations strategy and integration. By combining these vital functions under one DASD, the CIO has ensured that IA policies and procedures are consistent and complementary across various programs and disciplines. CIP efforts focus on the identification and characterization of the functions, systems, assets, supporting physical and cyber infrastructures, and interdependencies between the civilian and military sectors.

4. Critical asset prioritization and protection methodologies.
DOD does not use the Project Matrix review. It uses an Analysis and Assessment process developed and implemented by the Joint Program Office for Special Technology Countermeasures. The process is used to (1) identify critical assets; (2) identify the vulnerabilities of those assets, along with their interdependencies/interrelationships with other assets and infrastructures; (3) identify alternative solutions to the vulnerabilities; and (4) perform risk assessments. The IG did not identify or review a Project Matrix for DOD operations but reported on related areas. Contingency planning, for example, requires identification and prioritization of critical assets. As the IG report explained, contingency planning requires the Components to identify and prioritize their mission critical systems, but they have not effectively or consistently done so.

The DOD Critical Infrastructure Protection (CIP) Directorate has been working with the DOD operational community to develop the DOD Critical Asset Database. This database, not yet fully matured, will be structured to show critical capabilities and to prioritize critical sites by more than 100 possible asset combinations and query variations. The CIP Directorate also helped develop the joint National Imagery and Mapping Agency (NIMA) and the United States Geological Survey (USGS) city-mapping project. Together, NIMA and USGS mapped 154 cities throughout the United States to give emergency planners from the Federal to the local level an accurate critical asset picture. This information is essential for well-managed critical asset protection.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG did not identify or review DOD's overall progress in managing, reporting, and investigating security incidents during FY 2002. However, the IG DOD Report No. D-2002-093, "Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System," May 23, 2002, reported that the Defense Manpower Data Center's Noncombatant Evacuation Operations Tracking System was not compliant with the DOD Information Assurance Vulnerability Alert program. Corrective actions are ongoing. Included in these actions is the piloting of an enterprise-wide automated IAVA tracking system to ensure configuration management and compliance with directed security patches.

DOD has two primary documents that provide basic guidance for the agencies and Services to handle security incidents: DOD Directive O-8530.1,"Computer Network Defense," and DOD Instruction O-8530.2, "Support to Computer Network Defense." In addition, the DOD

CERT works closely with the Federal Computer Incident Response Center (FedCIRC) on all incidents within the .gov domain. The DOD CERT, as well as Service and agency CERTs share information with FedCIRC within ten minutes to 48 hours depending on the seriousness of the incident. The Joint Task Force for Computer Network Operations (JTF-CNO) and DOD CERT take responsibility for incidents within the .mil domain.

The Defense Criminal Investigative Service (DCIS) participates as a member of the Law Enforcement and Counterintelligence Center that DOD established to coordinate criminal and counterintelligence computer intrusion investigations and to disseminate relevant information to the military commands. The Defense Criminal Investigative Organizations (Army, Navy, and Air Force) reported computer crimes for the period from August 1, 2002 through July 31, 2002. Of 171 investigations initiated, 107 investigations closed, 20 indictments were made (with 10 indictments pending), and 17 convictions were made. The monetary recoveries from computer crime investigations for that period amounted to $49,103.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The Department reported that 352 of the total networks (241unclassified networks and 125 classified networks) were certified and accredited to operate, were assessed for risk and assigned a level of risk, and had up-to-date IT security plans.

In FY 2002, DOD reexamined 155 systems from the FY 2001 GISRA Report based on expiration of accreditation dates. This additional scrutiny from this year's review of the GISRA data has revealed and enabled correction of inaccuracies in initial interpretations of data fields and definitions and misinterpretations in data reporting in FY 2001. Some of these corrections resulted in lower percentages for FY 2002 rather than an actual decrease in performance**.** One hundred twenty five of the 155 systems were assessed for risk in FY 2001; 106 of the 155 systems were assessed for risk in FY 2002. In FY 2001, 125 of the 155 systems had been assigned a level of risk after a risk assessment had been conducted; in FY 2002, 106 out of the 155 had been assigned a level of risk. In FY 2001, 130 were reported as having an up-to-date security plan versus 103 of the 155 systems in FY 2002 being reported as having them.

DOD reported that 85 of the 155 systems are authorized for processing following certification and accreditation in FY 2002 and 70 are operating without written authorization (including the absence of certification and accreditation). Sixty two systems have the costs of their security controls integrated into the life cycle of the system. Forty three systems have had their security controls tested and evaluated in the past year. The Department reports that 103 of the 155 systems have a contingency plan and 32 of those systems have had the contingency plans tested in the past year.

2. Department methods to ensure contractor services are secure.

The IG did not review the status of contractor-provided services for compliance with GISRA or the Defense information Security Program. However, in summarizing DOD information assurance challenges reported from August 23, 2001 through July 31, 2002, the IG identified five reports that discussed weaknesses in background investigations. The Army Audit Agency evaluated the implementation of an entity-wide security program for the Corps of Engineers Financial Management System at three locations and issued three separate reports (Report Nos. A-2002-0251-FFC, A-2002-02550-FFC, and A-2002-0248-FFC) that identified and suggested improvements for completing district-wide background investigations for all employees. Additionally, the Air Force Audit Agency issued two reports (F2002-0046-EA0000 and F2002-0001-C06600) that identified weaknesses with background investigations. Both the IG and the Army Audit Agency plan to perform future reviews of this area in FY 2003.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG did not publish any reports that directly answer whether the agency CIO adequately maintains an agency-wide security program. However, the IG reported a number of systemic computer security and information assurance weaknesses in its information assurance challenges summary reports covering the period from January 1, 1995 through July 31, 2002. The IG noted that the Department improved IA initiatives by establishing the DOD Global Information Grid architecture, addressing IT interoperability, and addressing GISRA requirements using the DOD integrated process team. However, proactive efforts are still needed to lessen the risk to all interconnected DOD information systems and shared information; provide consistency in information assurance implementation; enforce accountability for implementing and managing information assurance requirements; and consolidate, revise, and implement information security policies to respond to the evolution of the network-centric infrastructure of DOD operations.

DOD reported that it provides Department-wide, component-level security training and periodic updates for all employees. However, actual numbers and percentage of agency employees, including contractors, who received security training in FY 2002 were not reported, although, the Department did report that $65.5M was spent on FY 2002 training. In addition to the IA and information security (INFOSEC) awareness training that is provided to all DOD employees, specialized security and technical training is provided to employees with special security responsibilities. Of 39,783 employees with significant security responsibilities, 16,812 received specialized training. DOD also is instituting a three-level IA certification program for System/Network Administrators (SAs), maintainers, and users. Most full-time SAs and Information Systems Security Officers (ISSOs) in DOD are certified through a combination of formal and informal security and technical training. Currently, DOD is also developing a certification process for Red Teams and computer crime investigators.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
The IG, Army Audit Agency, the Air Force Audit Agency, and the Inspector General of the Defense Information Systems Agency were unable to comment on whether DOD reported security requirements and costs on every FY 2003 capital asset plan or in the Exhibit 53 that was submitted due to insufficient time to exam the plans. DOD had not yet finalized its capital planning and investment information contained in its Exhibit 53 at the time of submission of its GISRA Report.

Department of Education (DOEd)

A. General Overview

1. Security funding.
The Department of Education reports planned FY 2003 funding for IT security and critical infrastructure protection of $20.6M. This funding level comprises 5% of their total planned IT portfolio of $410M.

2. Number of programs reviewed.
The Department instituted a semi-annual General Support System (GSS) and Major Application (MA) inventory revalidation procedure in FY 2002. This inventory procedure resulted in the review of the 18 agency programs and 92 agency systems. Every system owner completed a National Institute of Standards and Technology (NIST) self-assessment questionnaire.

3. Material weaknesses.
Both the Department and the IG reported numerous material weaknesses. Material weaknesses reported at the Department-level include: the need to identify security expenditures more accurately and completely; the inclusion of a full certification and accreditation process in the system development life cycles (SDLC); the need to fully integrate physical, personnel, and information security policies; revising its approach to conducting Critical Infrastructure Protection (CIP) actions based on Project Matrix; and improve the incident response capability with adequate funding and dedicated staff. System level material weaknesses were recognized in risk management, security controls, authorized processing, security plans, physical environmental protection, production input/output controls, contingency planning, hardware and system software maintenance, data integrity, security awareness and training, incident response, identification and authentication, logical access controls, and audit trails.

Across the Department's IT security program, 227 new security weaknesses were reported for FY 2002. Two hundred sixty weaknesses were carried over from FY 2001, for a total of 487 security weaknesses reported in FY 2002.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG determined that the Department successfully defined the responsibilities and authorities for the Secretary, the Department CIO and program officials in accordance with GISRA. However, the IG noted that the Secretary had not explicitly endorsed or approved the IT Security Program Management Plan and its program elements, which formally delegates to the CIO (or approved comparable official) the authority to develop and maintain an agency-wide information security program in accordance with the GISRA.

The Department indicated that the Secretary, through the support of the Deputy Secretary, has played an increasingly important role in IT security within the past year. The Department's report also stated that the Secretary and the Deputy Secretary will continue to oversee and implement specific security actions and undertake their GISRA roles and responsibilities, with the goal of making IT security an increasingly integral part of the Department's day-to-day business and culture. The Department's report falls short of confirming that the Secretary has delegated the responsibilities of IT security to the CIO as indicated in GISRA.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG noted that the Department continued to develop its certification and accreditation and security life cycle management programs to ensure that the Department's IT security plan, program, and practices are enforced throughout the life cycle of each agency system. Independent risk assessments conducted by the Department's contractor also revealed the Department's MAs and GSSs had not yet been certified and accredited to process information in accordance with OMB Circular A-130, Appendix III. The Department reported that all operating systems had begun a rigorous program to achieve certification and accreditation by December 2003. The Department placed priority on establishing a methodology for ensuring that security costs and considerations are evaluated at each stage of a system's life cycle.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The Department was in the process of developing a Communication Action Plan and Integration Action Plan to ensure successful integration of its various security programs including Critical Infrastructure Protection (CIP) responsibilities. The Department had designated different Principal Offices and officials to manage its physical, personnel, and various IT security programs. The IG reported that, because the various security programs had not been fully integrated, some program officials were not aware of the integration goals of the IT Security Program Management Plan and how it will impact their security programs.

The Department indicated that there had been increased coordination between Department staff to reduce duplication of security efforts. Coordination efforts include meetings involving personnel, physical, and IT security staff; coordination of joint input to policies; collaboration on plans and procedures that affect all Department staff; and the development

of new plans and procedures that specifically address integration. Both the IG and the Department reported that the IT Security Communication Action Plan will further enhance these integration efforts.

3. Critical asset prioritization and protection methodologies.
According to the IG, the Department was in the process of updating the CIP Plan to identify procedures designed to help the Department withstand cyber attacks on its key assets and to reflect its current operational environment. In addition, the CIO was conducting a Project Matrix Review to help: (1) identify and prioritize critical physical and cyber assets; (2) determine asset dependencies and interdependencies internal and external to the agency; and (3) evaluate critical assets and their supporting nodes and networks. The Department conducted the initial process of Project Matrix methodology by gathering Mission Essential Infrastructure (MEI) information for its cyber and physical assets. The CIO noted that, although progress had been made, additional work was needed to be completed in FY 2003 and concurred with the assessment of the IG.

4. Department documented procedures for reporting and sharing vulnerabilities.
According to the IG audit, the Department is developing an IT Security Incident Response Program Plan as a sub-element of the IT Security Program Management Plan's Continuity of Operations. The results of the IG's technical security testing indicated that the Department's incident response capability and its incident handling process needs improvement. Both the IG and the Department noted several incidents of unauthorized and unacceptable use of IT systems. The IG indicated that these weaknesses raise concerns regarding the Department's current incident response capability to detect, respond to, and report on computer security incidents in accordance with the Security Act. The Department's report acknowledged that there is still much to be done with managerial support, and the Department will significantly increase its operational readiness in this critical area.

The Department's Information System Security Incident Handling Guide documents specific procedures for reporting incidents to the Computer Security Incidence Response Team (CSIRT). The Incident Handling Guide requires sharing of incidents with GSA's Federal Computer Security Incident Response Capability (FedCIRC). All incidents are reported to the Department's CSIRT Manager within the Information Assurance Office. The CSIRT Manager determines whether FedCIRC reporting is warranted and notifies FedCIRC, if necessary. Any incidents that require the attention of law enforcement officials is referred first to the IG and the IG subsequently notifies law enforcement. Of the 18 agency components, 12 have incident handling and response capabilities. For FY 2002, three incidents were reported by the agency components and subsequently reported externally to FedCIRC or law enforcement.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The Department conducted system risk assessments of each of the 16 mission-critical systems the IG reviewed. The independent risk assessments identified security weaknesses

for the mission-critical systems in the areas of management, operational, and technical controls. Risk assessments also revealed that none of the 16 mission-critical systems reviewed were formally certified and accredited to process data in accordance with OMB Circular A-130, Appendix III. Risk assessment results indicated that 14 of the 16 systems did not have system security plans that meet the requirements of OMB Circular A-130, Appendix III, and NIST Special Publication 800-18. Additionally, results of the independent risk assessments had not been incorporated into the system security plans. The IG noted that the Department had not fully developed its certification and accreditation and security life cycle management programs to ensure that system security plans are practiced throughout the life cycle of each system.

The Department reported that they made progress in securing their systems. They acknowledged that there is room for further improvement and that risk management is an ongoing process that must be integrated in the daily business within individual program offices. Of their 92 systems, 100% had been assessed for risk and assigned a level of risk after the assessment. Thirty-nine percent had an up-to-date security plan in effect and none had been certified and accredited. Forty systems (43%) had a contingency plan, with only 27% of the plans being tested in FY 2002. The Department reported that no costs of security controls had been built into the life cycle of each system; however, these costs will be integrated once the Department's System Development Life Cycle Security Integration Guide has been fully updated.

2. Department methods to ensure contractor services are secure.
The IG reported concerns associated with contractor-provided services and whether these services met the requirements of GISRA, OMB policy, and NIST guidance. Specifically, there were four mission-critical systems on which the IG evaluated technical security controls and the IG noted several weaknesses and vulnerabilities displayed by the contractors. The Department utilizes the support of 24 contractor operations or facilities of which 15 were reviewed in FY 2002. The Department disagreed with the IG's assessment regarding the adequacy of security controls and will re-examine the IG's recommendation on changes to the currently used IT security designs.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
Significant progress in establishing a framework for developing an agency-wide IT security plan and program was identified by the IG report. The IG also noted progress in: establishment of goals and methodologies for ensuring compliance with security legislation, directives, and guidance; development and implementation of training programs for system risk assessments, development of system security plans, and requirement of system certification and accreditation. Additionally, the Department took significant steps towards identifying security risks associated with its major applications and general support systems. This was noted in the improvements displayed by: the Office of the CIO's development and implementation of a general support system and major application inventory guide; the

Office of the CIO's independent risk assessments of its major applications and general support systems.

However, the IG stated that the CIO must fully develop and implement many elements of its agency-wide IT security plan and program to ensure that IT security controls are practiced throughout the life cycle of each system. The Department also identified areas within the IT Security Program Management Plan that had not been fully developed and implemented. Additionally, the IG noted that critical documents and guidance related to the Department's Certification and Accreditation program had not been finalized. According to the IG's observation, "without the implementation of an effective agency-wide information security plan, program, and practices, the Department is unable to provide a consistent security posture that sufficiently protects sensitive and critical resources from unauthorized access or modification."

The IG reported that the Department had not fully developed elements of its IT Security Training Program to ensure that personnel with significant information security responsibilities fully understand the requirements of GISRA and other security legislation. Only 95 (2%) of 4,774 employees with significant security responsibilities received specialized training in FY 2002. FY 2002 IT security training costs increased three-fold over FY 2001 costs, from $80K in FY 2001 to $262.7K in FY 2002.

In accordance with OMB reporting instructions, the Department reported that they had adequately accounted for all known security weaknesses within the Department's Plan of Actions and Milestones (POA&M). The CIO appointed a senior agency information security official and is documenting applicable IT security responsibilities within the Department's IT Security Program Management Plan.

2. CIO methods to ensure contractor services are secure.
The IG reported that the Department CIO needs to develop procedures to determine whether contractor-provided services meet the requirements of GISRA, OMB policy, and NIST guidance. The CIO requires the review of all contracts dealing with IT systems. The reviewing official is tasked with ensuring that appropriate controls are in place to account for the security of information systems and data in external contracts. The request for proposal (RFP) for contractors cannot be released to the public without the express written authorization of the OCIO. Subsequent technical security review of systems run on contractor-operated facilities verifies compliance with these security requirements. Recent risk assessments and IG evaluation of four mission-critical systems revealed that compliance with applicable requirements is not consistent. The Department advised that their certification and accreditation program will include further technical reviews during the next year.

3. Agency integration of security and capital planning.
The IG's audit recommends that the Department fully develop and implement procedures for integrating security into its capital planning and investment control process. The IG noted that, although the Office of the CIO provided program officials with a new IT Security Cost Estimation Guide to identify system security requirements and costs, the resulting security

life cycle cost estimates had not been integrated into the IT Capital Planning and Budgeting process. The IG review also revealed that estimated system security life cycle costs were identified in certain detailed business case documents but were not summarized for the Investment Review Board for deciding on IT investments. The Department reported that 23 capital asset plans and justifications were submitted to OMB for FY 2004 and that all contained the requisite security information and costs. The Department also reported that all 23 plans and justifications were independently validated prior to submission to OMB.

Department of Energy (DOE)

A. General Overview

1. Security funding.
The Department of Energy reports planned FY 2003 funding for IT security of $127M. This funding level comprises 5% of their total planned IT portfolio of $2.5B.

2. Number of programs reviewed.
The Department is comprised of nine programs with 906 systems. The IG advised that they were unable to report on the number of Department systems to the level of specificity contemplated by OMB because, "at the time of our review, there was no all-inclusive inventory of the Department's systems." The IG reviewed 38 Department systems.

The program reviews and assessments were based on IT security policies and procedures of Departmental organizations as well as the Federal Information Systems Controls Audit Manual (FISCAM) and NIST 800-26, 'Security Self-Assessment Guide for Information Technology Systems'. For FY 2002, 66 program/system reviews were conducted utilizing the NIST 800-26 methodologies.

The Office of the CIO piloted the use of NIST 800-26 and promoted the use of the NIST Automated Security Self Evaluation Tool (ASSET) software program throughout the Department and is providing training on the use of this tool.

3. Material weaknesses.
The IG identified 69 separate IT weaknesses and recommended that management consider the overall effect of the problem when preparing its annual assurance memorandum on internal controls. The Department's remediation efforts and program initiatives in FY 2002 resulted in no findings of material weaknesses. Although numerous weaknesses were identified the Department indicated that they were not sufficiently serious to call for the establishment of a material weakness for the program. The Department is aware of the IG findings and is working to address them through changes in policies, procedures, and implementation of corrective actions.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG reported that, despite the reorganization of the Office of Security and Office of the CIO, the Office of the CIO does not review and approve program office and field sites' Cyber Security Program Plan (CSSP) updates. Additionally, despite the CIO's monitoring role, the CIO does not review the results of program-level cyber security assessments or evaluate the effectiveness of implementation efforts and policies. In the past, major operating components of the Department could make an IT investment decision without review by and concurrence of the CIO. However, with the Department's implementation of the Information Technology Investment Management Framework document, and the linkage of the Department's various IT management and control processes with the Capital Planning and Investment Control Process, the CIO is able to review and approve all proposed IT investment portfolios.

In the first quarter of FY 2002, the Office of the CIO was elevated to a staff office reporting directly to the Secretary. At the same time, cyber security authority was separated between the Office of Security and the Office of the CIO, with the assumption that overall improvement of IT security coordination would be attained. Office of Security was given responsibility for overall security policy and the Office of the CIO was charged with concentrating on policy implementation. The Office of the CIO implemented an IT capital planning and investment control process for its IT investments, which includes reviewing all IT investment budget submissions prior to going to OMB.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Department's increased focus on integrating security in the capital planning and investment control process has resulted in some improvements on the implementation of a life cycle approach to managing security. The Department, through the Office of the CIO, developed a POA&M database to track the status of IT security weaknesses identified by various reviews and evaluations. The CIO acknowledged that, despite these efforts, additional action is necessary to fully implement a life cycle approach to managing security. All critical computer assets have not been identified and prioritized, which is a first step to ensure that such assets are adequately protected. The CIO also acknowledged that, while the Department has committed to a risk-based approach to security planning and management, this process has not been fully implemented.

Under the Secretary's auspices, the Office of Security and the Office of the CIO were developing policy directives that will update and provide a greater level of consistency to the IT security roles, responsibilities, and requirements throughout the Department. The Office of the CIO began implementation of a pilot set of metrics in late 2001 that were aimed at measuring the implementation of key Department-wide elements of the IT security program. The CIO determined that the Department metrics embodied that of the OMB guidance and thus, the CIO has adopted the OMB metrics as a baseline for the Department.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The Department initiated an integrated approach to its critical infrastructure protection responsibilities, by implementing a Project Matrix review that will identify and prioritize the Department's critical assets and operations, including IT. A cyber security working group was established by the Department and includes the Office of Security, the Office of the CIO, and the National Nuclear Security Administration (NNSA). The NNSA is in the process of drafting separate IT security implementation guidance.

4. Critical asset prioritization and protection methodologies.
The IG noted that the Department had not yet developed an information systems baseline that included an inventory of applications and major systems in use or under development. Additionally, the IG reported that the identification of national priority assets had not been finalized and the specific identification of critical cyber-related assets had not begun.

The Department launched a Project Matrix review, but had yet to finalize the review. The Security Office is in the process of advising the Department's senior managers on the assets identified as national critical. Programs were initiated to evaluate physical and cyber security threats and implement mitigating measures. Initial results of Project Matrix systematically support the Department's identification of any additional critical assets and the potential reprioritization of existing critical assets. A certification and accreditation process is under development for unclassified systems that has enhanced requirements for national critical assets.

5. Department documented procedures for reporting and sharing vulnerabilities.
The Department requires all Departmental elements, NNSA, Program Secretarial Offices, and other Departmental organizations having access to Departmental IT systems to report IT security incidents to the Computer Incident Advisory Capability (CIAC). CIAC serves at the Departmental cyber incident reporting point of contact and, as such, assumes the responsibility of reporting IT security incidents to external organizations, such as FedCIRC, NIPC, and law enforcement. The IG expressed concern that there was no required average time for organizational components to report incidents to CIAC and, likewise, there was no required timeframe for CIAC to report incidents to FedCIRC. CIAC's FY 2001 Annual Report noted that only 47 of the 141 sites reported with a total of 47,813 incidents. In FY 2002, there were over 80,000 incidents reported to CIAC by DOE sites. Of those incidents, 164 were system compromises and the remainder fell into the category of scans and probes. CIAC estimates that the actual number of scans and probes was significantly higher; however, due to the large volume of scans and probes only those that appear to be a threat are reported to CIAC as an incident. While the number of incidents being reported continues to rise, CIAC acknowledges that many DOE sites are still not reporting incidents. The IG stated that "Without stronger reporting requirements, the Department cannot draw meaningful conclusions as to the effectiveness of it overall intrusion detection capability". The CIAC acknowledges receipt of reports of 80,567 scans. The Department believes it is no longer cost effective to record, report, and track the large volumes of probes and scans.

The IG's evaluation also disclosed vulnerabilities involved with the testing and installation of patches for applications and systems under each Departmental organization. Testing

performed at selected sites for the FY 2002 evaluation identified seven separate findings related to outdated software and uninstalled patches.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.

The IG was unable to provide a report on the Department's responsibility for risk because of the lack of all-inclusive inventory of systems and the IG evaluation only included a sample of the systems. The IG noted that network and individual system level security plans had not been prepared or were inadequate for most of the systems evaluated. The IG advised that the Department is in the process of developing guidance and training in the use of the NIST automated self-assessment tool that should enable the various Department elements to better assess the security controls of their various networks and systems.

The Department requires unclassified sites to have a Cyber Security Program Plan (CSSP), which requires the site to conduct and include a risk assessment as part of the plan. The IG concurred that each of the Department's programs and sited had prepared CSPPs; however, the plans generally concentrated on network assets and were not supported by risk assessments or addressed risk only in a generic manner. The Department reported that it has recently developed and is currently working through coordination of a new risk management directive. The directive is consistent with NIST and other national standards, and includes risk assessment, configuration management, and independent verification and validation components integrated into a mutually supporting process. Department policy requires unclassified plans to be updated every two years, unless a significant change takes place. The Department's capital planning process was improved with increased emphasis on ensuring that security is planned and funded throughout the IT life cycle. The Department reported that, since the enhanced processes for risk and configuration management, certification and accreditation, and independent verification and validation is currently in process, more testing and evaluation is needed.

2. Department methods to ensure contractor services are secure.

The IG expressed concern that program management, planning, and execution of IT security was a noticeable weakness in both contractor and federally run facilities. The Department makes extensive use of contractor provided services and of the Department's 126,330 employees, 110,000 are contract employees. Additionally, all but one of the Department's laboratories is contractor operated. The contractors are responsible for implementing the Department's IT security directives as specified in their contracts. Many of the contracts are performance based and incentives are tied to specific levels of achievement. The Department uses Program Office line management reviews, self-assessments, and peer reviews to provide feedback on the health of contractor IT security. The Office of Independent Oversight and Assurance (OA), the Office of the IG, and the Office of the CIO also provide information on contractor performance on IT security issues. The Department used 25 contractor operations or facilities during FY 2002 with 22 of these being reviewed.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.

The IG expressed concern over the lack of IT security protection efforts resulting from program management, planning, and execution weaknesses. The IG stated that the Department had been negligent in: consistent implementation of a risk-based IT security approach; assuring continuity of operations through adequate contingency and disaster recovery planning; strengthening incident response capability by reporting all computer incidents; ensuring employees with significant security responsibilities had received adequate training; and, adequately addressing configuration management and access control problems. The IG advised that these vulnerabilities existed because, "the Department had not strengthened its cyber security policy and guidance, implemented a cyber security performance measurement system, and established an effective self-assessment program."

The Department contends that several mechanisms have been established for maintaining an agency-wide security program. These mechanisms include the use of CIAC for incident response capability, CIO Operations for daily updates on the status of the Department's backbone, and the OA for the evaluation of Departmental policies and procedures and review of all security controls.

The Department's policy requires that personnel from all Departmental organizations and contractors be appropriately trained in IT security vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The Department stated that it funded various training sessions and sponsored several annual conferences concerning cyber security during FY 2002 at a cost of $1.7M. The Department also advised that 93% of employees and contractors in Program Offices or field sites were trained in FY 2002 at an estimated cost of $4M. The Department was unable to provide a training report progress for Departmental organizations because the organizations are not required to track and report progress in completing training for security personnel.

2. CIO methods to ensure contractor services are secure.

The IG and OA evaluations identified IT security weaknesses in areas of configuration management and access control, as previously identified elsewhere in this report. The Department reported no contractor operations or facilities were reviewed during FY 2002 that come under the CIO's direct control. The Office of the CIO's network operations team is responsible for providing a broad range of technical support services for the daily operation, maintenance, and administration of the backbone, attached systems and services used by all Headquarter organizations. Contractors who manage and operate the Department's networks and systems are held to the same level of accountability and system security review as those systems and facilities that are Federally operated. The CIO relies heavily on evaluations performed and provided by the IG and OA's Office of Cyber Security and Special Reviews.

3. Agency integration of security and capital planning.

The Department developed and implemented an IT capital planning and investment control process for its security investments. The Department indicated that this process will allow

for stricter adherence to requirements set forth in the Clinger-Cohen Act of 1996, OMB Circular A-130, GISRA, the President's Management Agenda, and OMB guidance in Circular A-11. The increased focus on cyber security considerations has resulted in improvements in the number of capital asset plans submitted to OMB from 15 for FY 2003 to 99 for FY 2004. The CIO's objectives of the IT investment portfolio process are to ensure that taxpayer dollars are managed wisely and effectively, and that security IT investments are results oriented and provide the necessary security and privacy protections.

Department of Health and Human Services (HHS)

A. General Overview

1. Security funding.
The Department of Health and Human Services reports planned FY 2003 funding for IT security and critical infrastructure protection of $138M. This funding level comprises 3% of their total planned IT portfolio of $4.75B.

2. Number of programs reviewed.
To identify an appropriate subset of systems to test, the IG relied on the Critical Infrastructure Assurance Office Project Matrix report. The IG reported that during FY 2002, the Department determined that approximately 500 systems were critical to day-to-day operations. The IG subset included the 30 critical information systems that scored high in any Project Matrix category.

The Department identified a total of 283 systems in FY 2002, of which 109 were reviewed. The Department indicated that a contributing factor to the number of systems reflected in the FY 2002 GISRA submission was the OPDIVs' more complete implementations and a more structured approach to inventories and accounting of critical assets. During FY 2002, each OPDIV used the NIST self-assessment guide or in-house developed methodologies that capture all elements of the NIST guidance in order to validate the systems supporting the agency's security programs.

3. Material weaknesses.
HHS reported one material weakness in FY 2002 that was a repeat finding from the previous fiscal year. The material weakness is an accumulation of findings at the Medicare fee for service contractor operations, as well as at the Centers for Medicare and Medicaid Services Central Office. The principal vulnerabilities were in the area of access controls, systems software and entity-wide security planning.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.

The IG reported that overarching technical management structure for IT security at the Department level is still in its early stages of development. A system security program for the Department and comprehensive list of systems need to be implemented so that all applicable IT assets across HHS are covered appropriately and effectively.

The Department reported on many initiatives and activities designed to improve oversight and monitoring of major Departmental risk factors. These efforts include: awarding a contract to conduct vulnerability assessments at all OPDIVs; authorizing the hiring of an entity-wide Chief Information Security Officer for a major OPDIV; leveraging the IT Security and Innovation fund established by Congress for Department-wide security initiatives; creating a Department-level security work group with representatives from each OPDIV; conducting regular CIO council meetings with a focus on security issues to help ensure compliance with Department-wide policies; increasing the attention to security criteria by IT investment review boards; and planning to award two Department-wide contracts to identify, document, and manage vulnerabilities and risk.

The Secretary mandated the development of a "One-Department" IT program which resulted in a comprehensive Enterprise IT Strategic Plan containing a major focus on security and critical infrastructure protection. HHS reported that the development, approval, and funding of this Plan played a major role in the subsequent direction of the Department's security strategies and activities. In addition, the Information Technology Investment Review Board comprised of the Department CIO, the OPDIV CIOs, the Department Chief Financial Officer, Deputy Assistant Secretary for Grants Management, Deputy Assistant Secretary for Personnel and the Assistant Secretary for Budget, Technology and Finance, played an important oversight roll for IT investments. The Board reviews and approves all significant IT investments. All OPDIVs reported that major IT investments required CIO review and authorization.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG's evaluation included an assessment of the OPDIVs' responses to OMB's performance measures. While they were found to be adequate representations of the various aspects of the security systems and program, for several of the OPDIVs, the IG was unable to verify management's responses to supporting documentation or some IG observations did not lead to conclusions similar to those of OPDIV management.

HHS reported that the Secretary requires that all OPDIVs ensure compliance with all federal laws and regulations, including best practice life cycle management security requirements. The One-Department Initiative and Five-Year IT Strategic Plan embody this approach for both program and IT management. The Secretary charged the CIO Council with responsibility for enforcement through the IT Investment Review Board process, program team progress reports and approvals, and program reviews. CIOs are held accountable through executive performance contracts and/or performance metrics, budget and financial reviews, reports and/or meetings.

The Department reported instituting standard performance measures to monitor the continuous reliability and availability of six critical IT infrastructure services on a 24x7 basis. These services include: Internet connectivity; HHS websites; e-mail services; HHS wide area networks; telephone dial-tone; and mainframe computing.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The Secretary designated a Critical Infrastructure Assurance Officer (CIAO) who is responsible for physical, personnel, and IT security. In addition, the Secretary integrated IT security and CIP Program responsibilities and assigned them to the Office of IT Security and Privacy. All OPDIVs integrated these responsibilities for their areas of authority to meet their specific needs. Within each OPDIV, IT security is coordinated closely with those responsible for personnel security, physical security, CIP, and Continuity of Operations.

The Department established a CIO Council, an IT Investment Review Board, and a Departmental Office of IT Security and Privacy to facilitate coordination, integration and minimize duplication of IT security efforts and procurements across all OPDIVs. OPDIVs have various authorities for different security functions (e.g., physical security under a facilities office, and IT Security under the CIO). All OPDIVs manage resources to eliminate duplication of effort and cost under normal operations.

4. Critical asset prioritization and protection methodologies.
All 13 OPDIVs have undergone a Project Matrix review, Identification and Ranking, for all critical infrastructure protection (CIP) assets. The Department completed Phase 2 for two of its most critical IT assets. In addition, HHS was in the process of awarding a contract before the end of FY 2002 to address critical infrastructure protection issues including: revalidating Project Matrix Phase 1 findings; conducting remaining Phase 2 analyses for HHS's most relevant CIP cyber assets; providing assistance in taking GISRA corrective actions on all most relevant CIP cyber assets; conducting certifications and accreditations on all most relevant CIP cyber assets; implementing a disaster recovery and continuity of operations solution for one of the most relevant CIO cyber assets; and updating the HHS CIP plan and Automated Information Systems Security Program Handbook to include CIP topics.

5. Department documented procedures for reporting and sharing vulnerabilities.
HHS policy requires that potential criminal activities be reported to the Computer Crimes Unit within the Office of the IG, which then reports as appropriate to external law enforcement and federal offices, e.g., FBI and FedCIRC. The policy also requires that these reports, as well as incidents that do not appear to be criminal in nature, be reported to the HHS Office of IT Security and Privacy and to FedCIRC.

The Department reported that it has commissioned an incident response and notification study and will use the results to formulate the next stage of the enterprise security program. In the interim, HHS established an in-depth emergency notification process and contact list of key OPDIV and Departmental security staff and CIOs across five security discipline areas.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
HHS reported that all OPDIVs began assessing risks for the operations and assets under their control. Of the 283 systems reported in FY 2002, 122 had been assessed for risk; 107 had an up-to-date security plan; 31 had been authorized for processing following certification and accreditation; 160 systems are operating without written authorization; 230 systems had the costs of their security controls integrated into the life cycle of the system; 95 systems had security controls tested and evaluated in the last year; 93 systems had a contingency plan; and 44 systems had those contingency plans tested in the past year.

2. Department methods to ensure contractor services are secure.
In FY 2002, HHS reported a total of 70 contractor operations or facilities, of which 59 were reviewed. Department program officials used NIST self-assessments, performance metrics, independent contractors for Independent Verification and Validation (IV&V), annual reviews, and software, such as the Contractor Assessment Security Tool (CAST) used by the Medicare contractors and the CMS data center. OPDIVs also have used the IT Investment Review Board to review application system business cases.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG evaluation found that most OPDIVs had not complied with OMB's instructions to prepare and submit a Plan of Action and Milestones (POA&M) for all programs and systems where a security weakness had been found. While all OPDIVs were using the POA&M as a management tool, only two were using it as the authoritative agency-wide management tool to prioritize, track, and manage agency efforts to close security performance gaps. The remaining POA&Ms were incomplete for one of the following reasons: failure to use in-house developed systems to track findings identified during various audits and program reviews as input source for the POA&M; absence of a process to identify and address security weaknesses; OPDIV belief that ongoing security assessment is an operations and maintenance activity that should not be tracked; and OPDIV belief that POA&Ms should include only weaknesses associated with non-financial systems.

The Department's specialized IT security training expenditures increased from $385K in FY 2001 to over $1M in FY 2002, while the number of computer security staff increased from 234 in FY 2001 to 318 in FY 2002. Annual department-wide security awareness training for all staff was institutionalized, whether using internally developed materials, or other effective practices from industry. The Department's awareness programs were also independently reviewed and validation as conforming to industry standards. Tracking of completion statistics was enhanced in all OPDIVs to meet reporting requirements.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
HHS indicated that it has fully integrated security into the agency's capital planning control process for all IT projects within its Five Year IT Plan.

Department of Housing and Urban Development (HUD)

A. General Overview

1. Security funding.
The Department did not provide the requested information pertaining to the FY 2003 budget request. Security funding for HUD was not consolidated during the timeframe of this report. Funding was in numerous areas such as program office project submissions, the COOP program and IT specific security infrastructure projects.

Based on the Department's submitted IT budget materials, OMB estimates FY 2003 IT security spending of $ 5.6M out of a total IT budget of $354M.

2. Number of programs reviewed.
The Department reported that they operate one program and 127 systems, of which 75 were reviewed in FY 2002. These 127 systems were analyzed for system weaknesses and reporting of performance measures. The Department used the NIST 800-26 self-assessment guide for the FY 2002 annual reviews.

3. Material weaknesses.
The IG found that many reviews lacked adequate supporting documentation and written clarification of mitigating factors. Additionally, the IG is in disagreement with the Department's overall assessment of the Department's status. The IG stated that persistent weaknesses were reported in (the Department's) general controls along with continued deficiencies in the agency networked environment. Further, the Department failed to report 17 new weaknesses documented by the IG in their FY 2002 audit. The Department reported seven program and 1,002 system material weaknesses for FY 2002. Sixty-nine system weaknesses were repeated from FY 2001 while no program weaknesses were carried over. The IG is of the opinion that the representation of the self-assessments is inaccurate and may lead to erroneous conclusions.

The seventeen findings were rolled up under Network Security Assessment and reported as one weakness in the Department's GISRA report. The 17 findings were all closed in October of 2001 as noted in the Departmental Automated Audits Management System, Audit Number 2002-DP-0001 with Report Date of July 11, 2002.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.

The Secretary used established methods to ensure the responsibilities in GISRA are being enforced. In addition, the Secretary placed great reliance on the President's Management Agenda Scorecard Reporting. This reporting process lists the responsibilities, goals, and projects of the Assistant Secretary for Administration and CIO. All IT issues come under the mission of the Office of the CIO, and this ensures that no IT investment decision can proceed without the concurrence of the CIO. The Department management feels that since the enforcement responsibilities lie within the Assistant Secretary for Administration and CIO auspices, there is no need for formal, overt procedures. That combined with the ongoing reporting, IG audits, and the annual GISRA review all draw frequent attention for the Secretary to the responsibilities for Agency officials.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG evaluated the Department's security plans program in October 2001 and determined that systems with security plans were found not to be in compliance with OMB A-130 or the NIST guidance. The Department is of the opinion that responses to the NIST self-assessment questionnaire indicate the agency is largely effective in following security plans throughout the life cycle of its IT systems.

While the IG has oversight authority within the Department, the Clinger Cohen Act states that the CIO is responsible for monitoring the performance of information technology programs of the agency, evaluating the performance of those programs on the basis of the applicable performance measurements, and advising the head of the agency regarding whether to continue, modify, or terminate a program or project. The IG states, "(The Department's) information system security program, like any other IT program must have executive level leadership, direction, and control to be effective and successful." The Department's response indicated that outside of the preparation and review of the POA&M reports to OMB, the only ongoing oversight process in place to ensure compliance with the requirement to practicing security planning throughout the life cycle of Department IT systems are audits performed by the IG.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The IG found little progress had been made by the Department to implement the activities/initiatives outlined in the Critical Infrastructure Protection (CIP) Plan. The Secretary authorized that the CIP Support Initiative be part of the Office of the CIO's mission. This major security initiative has already simplified the security budget for the Department as it is centrally managed from one organization, the Office of the CIO. The IT security organization as part of the Office of the CIO will plan, manage, and oversee the cyber security program.

HUD modified the CIP plan to comply with PDD-63. Work commenced and was ongoing for the Training, Incident Response, A-130 Review, System Security Policy and Plan Review, and Risk Assessments initiatives as outlined in the CIP plan.

4. Critical asset prioritization and protection methodologies.

The Department performed an annual review and update of security plans for systems. While this did not provide an overarching managerial view of assets and security, it did provide a lower level view that ensures IT security issues are being thought of and addressed. The Department has, in the past, identified and maintained lists of critical operations and assets with interdependencies and interrelationships. These were developed based upon the subjective mission goals of the Department and to meet crises. In FY 2002, the Department did not have a fixed, formal mechanism for identifying its critical operations and assets, their interdependencies and interrelationships, or procedures for how they secure all of their operations and assets. A Project Matrix review is scheduled for FY 2003 and formal briefings had been held between the Project Matrix team and Departmental representatives to discuss the scope and significance of the review. The Department is in the process of gathering documents for submission to an account manager who has been assigned to the Department from the CIP Office.

5. Department documented procedures for reporting and sharing vulnerabilities.
The Department developed a Computer Incident Response Program (CIRP) for reporting security incidents and sharing information regarding common vulnerabilities. The CIRP was specifically written to adhere to requirements mentioned in OMB Circular A-130, Appendix III. The CIRP document includes procedures, instructions and incident response forms, contact lists, and a Computer Intrusion Complaint form for the FBI.

The CIRP is documented and the contract award was pending. A phased implementation is planned and was to begin in October 2002. The Department had not yet defined "timeliness" of cyber security incident reporting as it pertains to the Department.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The Department is in the process of establishing Senior Security Manager positions for all program areas. Pending approval, the Security Managers' roles have been proposed to be assigned to the Continuity of Operations (COOP) managers. The Managers' roles will be to serve as the focal point for their program or division that will coordinate all security related matters and issues for their programs with the Office of the CIO. They will increase program officials' involvement in security and provide for additional accountability. Security management roles delegated to staff on the Program Management Review Board.

The IG reported that they had not been able to corroborate the results by the Department. Of the 127 agency systems, 124 or 98% had been assessed for risk. Eighty four percent of the systems have an up-to-date security plan and 100% have a contingency plan in effect. All of the systems have had the contingency plan tested within the past year. Ninety two of the total one hundred twenty seven systems have been certified and accredited.

2. Department methods to ensure contractor services are secure.
All cyber related contractor services and products fall under one Department program. The Department reported that contractor security is ensured through IG audits, in-place

inspections, and in some cases, continuous surveillance over contractor services and products. Periodic reports on contractor security performance are provided to the Assistant Secretary for Administration.

The Department reported only one contractor operation or facility and this contractor was reviewed in FY 2002.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that little progress had been made towards the completion of initiatives designed to strengthen the Department's IT security program. The IG anticipated improvement in this area in the next fiscal year. The Department CIO developed an Information Security Plan (ISP), which provides details on the agency-wide security program. The ISP was undergoing review and revision, but the Plan had not yet been fully implemented

FY 2002 employee and contractor training had been non-existent as the CIO contends that reliance on the normal contracting process of the Department has slowed the process. Of the 12,300 employees and contractors of the Department, none had received IT security training for FY 2002. The Department reported that, of the 150 employees with significant security responsibilities, 50 had received specialized security training. No costs were associated with the training as the limited training that had been provided was through in-house governmental staff. The IG provided no comment to this question.

2. CIO methods to ensure contractor services are secure.
Same as C.2.

3. Agency integration of security and capital planning.
The Department advised that they are integrating security into the capital planning and investment control process and that applicable documents and submissions will address security requirements and costs as reported in FY 2003 capital asset plans. For FY 2004, 48 capital asset plans and justifications were submitted to OMB following independent validation by the CIO and other appropriate officials. Security costs were included in all of the Department's IT systems. The IG concurred with the Department's response.

Department of the Interior (DOI)

A. General Overview

1. Security funding.

The Department of Interior reports planned FY 2003 funding for IT security and critical infrastructure protection of $34M. This funding level comprises 4% of their total planned IT portfolio of $852M.

2. Number of programs reviewed.
Both DOI and the DOI IG reported that the lack of a credible DOI IT system inventory casts doubt on the accuracy of various statistics and performance results contained in the DOI FY 2002 GISRA submission. With this caveat in mind, DOI evaluated aspects of its IT security program management in all ten of the component program areas, including financial and Indian Trust management and reviewed selected IT systems in each area. DOI reported a total of 37 programs in FY 2002, of which six were reviewed and a total of 224 systems, of which 58 were reviewed in FY 2002. DOI used the NIST SP 800-26 methodology for these reviews.

3. Material weaknesses.
Although progress had been made in implementing and maintaining an information security program and strengthening security controls and techniques, the IG found that DOI and its Bureaus' information security policies, procedures, and practices were not in compliance with federal requirements and therefore, DOI should continue to report a material weakness in computer security.

In FY 2001, DOI reported five material weaknesses and seven in FY 2002. Five of the FY 2002 material weaknesses are repeat findings. DOI's Management Controls Council reported that IT security was a material weakness, with failures in several specific areas: policy standards, certification of IT system plans, testing contingency plans, incident handling, training, and funding of IT security throughout an IT system life cycle. The Department has placed a high priority on its IT security function and has organized an effort for continuous monitoring of program achievement level via an expanded corrective action plan.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG indicated that the Departmental CIO did not have a direct report to the Secretary during FY 2002. In addition, program officials, such as the Assistant Secretaries and Bureau heads, deputies, and assistant directors have not been held accountable for carrying out their responsibilities and authorities as defined under GISRA and the Clinger-Cohen Act. These activities include ensuring all systems supporting operations and assets under the program officials' control have up-to-date security plans that are practiced throughout the life cycle of each system.

During FY 2002, DOI designed a formal process to review and approve IT investment decisions.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported that the Secretary designated the Associate Deputy Secretary responsible for overseeing all aspects of the DOI IT management program. In addition, in August 2002, the Secretary issued a memorandum stating that IT security was a top DOI priority and established the IT Management Council. However, the IG reported that the Secretary needs to take further action to oversee the performance of program officials to ensure that the IT security program and IT security plan are implemented; that those plans are up-to-date and practiced throughout the life cycle of each system, and that program officials identify all IT systems under their control.

The CIO adopted an annual Bureau-level IT Security Plan process developed by Fish and Wildlife Service as a best practice for Department-wide implementation. The CIO also prepared General Support System and Major Application guidelines and templates for System Security Plans based upon NIST guidance. In addition, the CIO adapted Rules of Behavior guidance developed by the National Park Service to be used as a best practice. DOI was developing a Departmental certification and accreditation process, which is based upon NIST Special Publication 800-37, for implementation during FY 2003.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG indicated that the DOI IT security program was not well integrated with critical infrastructure protection responsibilities. The Office of Law Enforcement and Security has staff responsibility for the DOI critical infrastructure program and for personnel, physical, and operational security Department-wide. While progress is being made to correct weaknesses, specific steps to eliminate unnecessary duplication of overhead costs and to ensure that policies and procedures are consistent and complimentary across DOI requires further work.

DOI reported that during the FY 2002 GISRA reporting cycle, the integration of its critical infrastructure and IT security functions was set into motion. A new Deputy Assistant Secretary position was created and filled to direct Interior's Office of Law Enforcement and Security (OLES) programs nationwide. This restructuring assigns OLES as the policy and information flow coordinator between the Department, law enforcement and the security staff of the Bureaus. Working with the Office of the CIO, the new OLES has created policy and procedure guidance on these security areas in four Departmental manuals.

4. Critical asset prioritization and protection methodologies.
DOI had not undergone a Project Matrix review by the national Critical Infrastructure Assurance Office (CIAO). (The Department CIO is working with the DOI CIAO to coordinate a Department-level Project Matrix review during FY 2003.) In FY 2002, DOI used an alternative process, based on Presidential Decision Directive (PDD) 63 criteria, to identify national critical infrastructures and systems. However, the Bureaus did not implement the DOI Critical Asset Valuation Guideline and DOI did not complete its enterprise architecture or ensure that all IT systems are identified. Consequently, the relationships and interdependencies with the IT systems and supported operations and assets

cannot be accomplished. Therefore, DOI has little assurance that all of its critical operations and assets have been identified and that the appropriate security technologies have been implemented.

5. Department documented procedures for reporting and sharing vulnerabilities.
DOI updated a number of its policies and procedures to better assist the Bureaus in identifying, reporting, and escalating incidents to appropriate levels of management and law enforcement authorities and to share common vulnerabilities with FedCIRC and with DOI components. However, the IG noted that only four Bureaus had established the required policies. Further, the DOI policy needs to be improved to ensure that unsuccessful or low level incidents are reported and tracked and that responsibilities for reporting and sharing all incidents are clarified.

DOI reported that of a total of ten components, nine have incident handling and response capabilities and report to FedCIRC in a timely manner consistent with FedCIRC and OMB guidance. However, there is currently no Departmental process in place to ensure that patches have been tested and installed in a timely manner. The CIO is reviewing some processes in place in the Bureaus for best practices for possible adoption Department-wide.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
DOI program officials did not assess the risks and determine the appropriate level of security to adequately protect all IT systems. The IG reported that although some systems had been assessed, the risk assessments were generally inadequate because not all interconnections with external systems were included in the assessment. Further, the Bureaus were not able to adequately manage risks for systems and supporting operations and assets because they have not yet identified all systems. Without risk assessments, DOI and Bureaus cannot determine the appropriate level of security needed to protect IT systems and supporting operations and assets.

DOI reported that 42 of its 224 systems had been assessed for risk. Seventy systems had an up-to-date security plan. Of the 224 total systems, 49 had been authorized for processing following certification and accreditation, leaving 175 operating without written authorization

In addition, DOI reported that 109 systems had the costs of the security controls integrated into their life cycles. The Department indicated it tested or evaluated the security controls of 51 systems in the last year. Also, DOI reported 63 systems had a contingency plan, of which 23 had been tested in the past year.

2. Department methods to ensure contractor services are secure.
The IG noted that DOI's IT Security Program and IT Security Plan require that appropriate language be included in contracts and memorandums of agreement or understanding for IT operations, but that program officials had not ensured that appropriate language was included in all IT service providers' contractual agreements. Findings also indicated that program

officials had not ensured that the IT service providers had adequate security controls that met federal standards. The Department considers this area to be a weakness in its overall IT Security Program and will focus particular attention on improving it in FY 2003.

The IG further reported that at least three Bureaus that use service providers receive reports related to the internal controls of the service providers' IT environment. While not specifically related to IT security, these reports address security issues such as controls over the operating systems, access procedures, and separation of duties.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG noted that all policies and guidance were not implemented by the Bureaus. All systems were not identified, certified, accredited, and authorized to operate. Procedures were not developed to validate whether all Bureaus have effectively implemented federal and DOI IT policies, procedures, standards, and guidelines. In addition, procedures were not established to keep DOI IT security policies and guidance up-to-date.

The IG also reported that for the first time, the DOI CIO ensured that all DOI employees and contractors had access to IT security awareness training and that procedures were established to document training results. The Department indicated that employee and contractor security education and awareness training that was once previously neglected and often overshadowed by operational demands, is now the cornerstone of its new IT security strategy.

The Department revised the IT Security Program and IT Security Plan, issued interim guidelines and technical bulletins to improve DOI's overall security program, directed the IT Security Team to address DOI-wide IT security weaknesses, required Bureaus to provide the information required under GISRA, and required Bureaus to provide plans of action and milestones for correcting IT weaknesses. However, additional work needs to be done before an adequate DOI-wide security program is maintained, implemented and evaluated.

DOI acknowledged the possession of more IT systems than are individually identified in its budget (Exhibit 53) and that it does not have a credible IT system inventory. DOI has set a goal of completing an inventory and prioritizing systems by the first quarter of FY 2003.

2. CIO methods to ensure contractor services are secure.
The IG reported that the Department revised the IT Security Program and IT Security Plan to require appropriate language is included in contracts and memorandums of agreement or understanding. However, the Department did not ensure that program officials included the appropriate language in contracts for IT operations and software development and maintenance. In addition, the Department did not ensure that the contract for one system under the control of the Office of the CIO had the appropriate contract language to ensure that federal IT security requirements were met. DOI is aware that this is a weakness in its overall IT security program and has already begun to focus attention on improving it. The

issue was a featured agenda item in DOI's recent IT Security Summit. It will receive extra emphasis during FY 2003.

3. Agency integration of security and capital planning.
The IG noted that although the FY 2004 IT capital asset plans included security requirements and costs, all security requirements and costs may not be known because the Bureaus had not performed adequate risk assessments including risk assessments for systems under development and evaluated and tested security controls.

For the FY 2003 capital planning and investment control process, the integration of security requirements and costs was not accomplished. However, for the first time, for the FY 2004 budget submission, DOI established a formal process for IT capital planning. As part of the new process, the CIO's IT Security Program Office staff reviewed the IT capital asset plans to assure that security requirements and costs were included and adequate. In addition, DOI's IT Security Team now is working with the Department's Enterprise Architecture Team to ensure IT security program principals are integrated into DOI's IT Enterprise Architecture.

Department of Justice (DOJ)

A. General Overview

1. Security funding.
The Department of Justice reports planned FY 2003 funding for IT security and critical infrastructure protection of $223M. This funding level comprises 11.7% of their total planned IT portfolio of $1.9B.

2. Number of programs reviewed.
The IG selected a different subset of systems within the Department to review in FY 2001 than in FY 2002. In FY 2001, the IG reviewed the following Justice components: Bureau of Prisons (BOP), Drug Enforcement Agency (DEA), Executive Office of U.S. Attorneys (EOUSA), Justice Management Division (JMD) and the Federal Bureau of Investigations (FBI). In FY 2002, the IG reviewed the Immigration and Naturalization Services (INS), Office of Justice Programs (OJP), U.S. Marshal's Service (USMS), FBI, and BOP.

The Department reported 26 agency programs, all of which were reviewed in FY 2002. DOJ also reported 275 systems, of which 209 were reviewed in FY 2002. Department components conducted self-assessments on 168 systems, approximately 80 percent of all sensitive but unclassified (SBU) systems, using the National Institute of Standards and Technology (NIST) Automated Security Self-Evaluation Tool (ASSET) distributed to agencies in July 2002. The FBI is in the midst of certifying and accrediting its systems and consequently, did not participate in conducting self-assessments. It recently recertified and accredited five SBU systems. The FBI is focusing its resources on completing risk

assessments for the remainder of its SBU systems and on completing the certification and accreditation (C&A) process for its national security systems.

3. Material weaknesses.
In its FY 2001 Accountability Report, DOJ identified computer security as a material weakness. New Departmental policy issued in July 2001 facilitated completing designated corrective actions and the Department closed this material weakness. However, DOJ continues to recognize computer security as a serious and pervasive issue and as a result, it is again declaring it a material weakness, with plans to provide an updated and expanded corrective action plan.

In FY 2002, the IG identified material weaknesses in the following 10 areas (asterisked items reflect repeat material weaknesses previously identified in the FY 2001 GISRA review): data integrity, audit trails*, authorized processing (C&A), contingency planning*, hardware & software maintenance (system patches)*, risk management*, logical access controls, password management*, review of security controls, and system security plans.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
In April 2002, the Attorney General (AG) appointed a new Chief Information Officer (CIO) to implement the AG's IT strategic plan, which includes ensuring that internal and crosscutting component problems are not repeated from year-to-year and not found within different components. The AG also revised the Department's initial strategic plan to incorporate additional security goals, including IT security. In addition, the Department was proposing reorganization of its IT program that will elevate the role and importance of security and clarify lines of responsibility and accountability. The proposal designates a senior information security official and establishes an IT security staff reporting directly to the Department's CIO. The IG reported that at the time of its review, the CIO was newly on board and the strategic plan was being deployed and OIG therefore was unable to test the implementation, enforcement, and effectiveness of the AG's actions.

At the time of the IG's review, major Department components could make an IT investment decision without the approval of the DOJ's CIO for non-major investments. The IG is concerned that being able to make investment decisions without the Department CIO's approval may allow the component to redirect funding to other projects. If the funding is inappropriately spent, these investments may not be disclosed until the following year's budget review. In August 2002, DOJ initiated a study to refine the IT investment management (ITIM) process. The study focuses on creating an integrated Department process that is linked to component-level ITIM processes and on establishing a systematic and effective Departmental oversight process for reviewing and assessing IT projects throughout their life cycle. Upon completion of the study in December 2002, recommendations will be incorporated into the Department's overall ITIM process.

The CIO approved seven of eight components' ITIM processes and had planned to approve the remaining one by September 30, 2002. The ITIM processes include various levels of approval within the components for individual IT investments based upon the business case and/or dollars of the investment, with senior management review and/or Department CIO review occurring on major investments.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Department attempted to ensure that an information security plan is practiced throughout the life cycle of DOJ systems through its C&A process. The IG found that the Department had inconsistently enforced its C&A policy. Three of five sensitive but unclassified systems (SBU) and one of three classified systems had incomplete C&A documentation. Systems development life cycle methodologies employed during FY 2002 were inadequate and did not include IT security measures throughout the system's life cycle as required by Department policy. The IG reported that these findings point to problems at both component and Department levels. The components had not followed existing Department guidance in the areas of contingency planning, security testing and the development of system security plan. In addition, the Department had not adequately performed oversight and monitoring of accredited systems.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG reported that the Department integrated its IT program with the critical infrastructure program (CIP). In addition, the Department's IT strategic plan includes initiatives for designing and implementing a Department-wide Public Key Infrastructure.

Separate staffs have been responsible for different aspects of the Department's IT security responsibilities. In FY 2001, the IG expressed concern for fragmented responsibility and resources and recommended consolidation. At the time of its FY 2002 review, no special efforts had been implemented to alleviate duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines. Since the IG review, the Department CIO informed the IG of its proposal to reorganize its IT security oversight in concert with the IG GISRA FY 2001 recommendation. The proposed reorganization would permit DOJ IT security oversight to concentrate resources (time, funding, and expertise) in order to more effectively identify and monitor the correction of system security vulnerabilities.

4. Critical asset prioritization and protection methodologies.
Although the Department had not used the Project Matrix Review methodology, it performed reviews using a methodology similar to the Project Matrix Review to identify critical operations and assets. DOJ attempted to secure its systems by addressing vulnerabilities identified through the Department's C&A process and through the performance of system tests to determine if security controls are in place. The Department also modified its critical assets selection process to consider the impact on the Department's ability to conduct its Presidential Decision Directive (PDD) 63 activities if assets were lost for 72 hours. (The PDD 63 activities focus on protecting the Nation's critical infrastructures from both physical

and cyber attacks.) The IG concluded that the methodology used by the Department is sufficient for identifying critical operations and assets.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG found that for four of the five SBU and two of the three classified systems, the components did not always monitor, track, and report incidents as required by DOJ policies. Some components were found to lack knowledge of the formal incident response procedures and personnel resources to ensure that incidents were properly reported. IG findings also indicated that one of the five SBU systems and one of three classified systems did not have up-to-date system patches installed.

The Department's DOJ Order 2640.2D requires components to report security incidents to the DOJ Computer Emergency Response Team (DOJCERT). This emergency response team is responsible for reporting these incidents to FedCIRC within 30 hours after being notified that an incident occurred. The Department's Security and Emergency Planning Staff (SEPS) is responsible for coordinating and reporting classified and national security information systems incidents to the National Infrastructure Protection Center and the Intelligence Computer Incident Response Center. However, SEPS has the discretion to withhold such information regarding security incidents of this type from the Federal Computer Incident Response Center (FedCIRC). For incidents involving criminal actions, the information is reported to the FBI. Incidents caused by external influences are reported to the National Infrastructure Protection Committee (NIPC) and FedCIRC. For any incident that affects more than one component, DOJCERT is required to share this information with components. DOJCERT shares this information with the components by sending out a "Security Alert" with details of the incident(s) and suggestions for prevention. According to DOJCERT, the Department reported 56,870 incidents in FY 2001 and 114,738 in FY02.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
Of the eight Department systems the IG reviewed in FY 2002, all had undergone reviews in the past in compliance with Departmental policy, but were found by the IG to have weaknesses associated with risk management. Specifically, system security plans were either incomplete, outdated or both. At the time of its review, the IG found that the Department did not have a centralized tracking system for these vulnerabilities that would ensure that corrective actions were taken. The Department reported that it developed its SMART database to track security weaknesses and planned corrective actions identified through the C&A process and in other security reviews such as IG audits and penetration tests. Demonstrating its commitment to track system weaknesses and corrective actions, DOJ reported that it expanded SMART to include 156 systems this year. The database also is being modified to allow components to update their system data and track their own system security status.

2. Department methods to ensure contractor services are secure.

The IG review found that inadequate steps were taken to ensure that contractor personnel were held to the same security standards as component staff for SBU and classified systems. Security program officials for two of the five SBU systems did not take adequate steps to ensure contractor personnel met the same security standard as component employees. For one system, all component employees were required to sign a "Rules of Behavior" document governing the use of the systems; however, contractor staff members were not required to sign it. For another system, the IG found that no "Rules of Behavior" document existed, although it was required. In addition to better enforcement of existing policy regarding methods to ensure contractor services are secure, the Department plans to adopt standard Federal Acquisition Regulations language on IT security that is currently under development.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that Department Order 2640.2D lacks specific security awareness training requirements for system administrators and security administrators different from those required for general users. In addition, most of the Department's security awareness and training requirements are focused on government employees, not contractors. The Department is aware of these deficiencies within its policy, and the newly appointed CIO focused on updating Department policies as part of the IT strategic plan. In FY 2003, DOJ will implement a Web-based security awareness product to distribute training to users' desktops Department-wide. The product will be used for contractor personnel, as well.

The IG component reviews also found that existing Department training policies were neither followed nor enforced. In addition, the IG found repeats of previously identified vulnerabilities, highlighting the lack of accountability at the component level and the lack of consistent monitoring through the C&A process by the Department.

2. CIO methods to ensure contractor services are secure.
See number C.2.

3. Agency integration of security and capital planning.
The IG and the Department reported that security has been integrated into the Department's capital planning and investment process. DOJ's Information Technology Investment Management (ITIM) process follows OMB guidance, the Clinger-Cohen Act, and other statutory provisions affecting IT investments. IT security is one of the strategic investment criteria used by the Department to prioritize Department investments.

Department of Labor (DOL)

A. General Overview

1. Security funding.

The Department of Labor reports planned FY 2003 funding for IT security of $78M. This funding level comprises 17% of their total planned IT portfolio of $443M.

2. Number of programs reviewed.
The Department reviewed 13 programs with 46 systems. Five systems that were reported in FY 2002 have been consolidated into other systems. The Department indicated that 36 additional systems were identified in FY 2002 as having sensitivity issues and will be reviewed during FY 2003.

3. Material weaknesses.
The IG's examination of the FY 2002 subset did not identify any material weaknesses. However, the IG review of this area revealed system security vulnerabilities and other weaknesses as follows: entity-wide security program planning and management; access controls; application software development and change control; system software; and service continuity. Three significant vulnerabilities were assessed by the IG: 1) information existed on the public Internet that could enable a malicious user to learn sensitive information about the system; 2) account with administrator-level privileges had an easily guessed username and password that could enable a malicious user to compromise the integrity of the system; and 3) password policy and settings contributed to the overall control breakdown of the system. The Department reported no material weaknesses in accordance with OMB Circular A-123. They indicated that those weaknesses identified were of lesser significance and are addressed in the Plan of Action and Milestones (POA&Ms).

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG reviewed specific areas of CIO responsibility, namely IT management, information management, and information security. The Department implemented CIO performance measurements that are tied directly with the GISRA, E-Government performance, and the Government Performance and Results Act (GPRA). Specifically, the CIO is responsible for: 1) ensuring that the Department's IT Security Plan is practiced through the life cycle of each system and 2) developing an IT Security Plan that ensures the Department implements and maintains IT security policies, procedures, and control techniques, trains personnel with significant IT security responsibilities, and assesses the IT security risk associated with operations and assets of the programs and systems.

The CIO is also part of a departmental review and decision-making process for formulating recommendations regarding IT policy, capital investments, and information resource management.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG's review during FY 2002 revealed that 14 of 16 systems they evaluated had a security plan in effect. Eleven of the 14 systems had an up-to-date security plan. The IG identified specific security areas that were not completely addressed, including: (1) change control

policies and procedures, (2) access to software libraries, and (3) development and updating of critical system documentation. Consequently, even though the security program has been fully integrated within the Department's System Development Life Cycle Manual (SDLCM), it has not been fully integrated within the systems.

The Department indicated that their security program had been fully integrated within the Department's SDLCM. This includes the incorporation of the certification and accreditation process, risk assessments, system security plan development and contingency plan development during the appropriate phase of the system life cycle. The Secretary oversees the performance of program officials and the CIO by linking their performance with E-Government security objectives, the President's Management Agenda, and GISRA. Additionally, the CIO conducts quarterly capital planning reviews, provides outreach and assistance, and periodically conducts facilitated sessions and conducts post-reporting reviews.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

According to the IG's independent audit, each of the seven component agencies had officials designated as security officers. However, audits on specific Department financial and financial-related systems identified that there are several weaknesses that would impair the Department's ability to effectively respond to a disruption in business operations as a result of a disaster or another event. The IG's independent review of four bureaus' POA&Ms validated that there were 13 weaknesses and corresponding corrective actions in the area of continuity of operations. The Department reported that it is implementing a comprehensive and coordinated critical infrastructure protection strategy that includes both cyber and physical security. The Department also established an integrated approach encompassing Department- and agency-level responsibilities and initiatives. Additionally, the Department continued to revise and update its Continuity of Operations Plan in order to minimize any disruption of essential mission and functions that support the U.S. economy and workforce.

4. Critical asset prioritization and protection methodologies.

The IG's and Department advised that a Project Matrix Team did issue a report to the Department concerning the completion of Step 1 of a Project Matrix review. They also reported that none of the six candidate assets met the criteria for a Step 2 analysis and, thus, considered the effort closed. Step 1 of the Project Matrix review was completed in FY 2002.

5. Department documented procedures for reporting and sharing vulnerabilities.

The IG reported on 7 agency components, with all having incident handling and response capability. During FY 2002, 34 incidents were reported with 4 being reported externally to FedCIRC or law enforcement. The IG's assessment resulted in the identification of 3 significant security vulnerabilities: 1) information existed on the public Internet that could enable a malicious user to learn sensitive information about the system; 2) accounts with administrator-level privileges had an easily guessed username and password that could enable a malicious user to compromise the integrity of the system; and 3) password policy and settings contributed to the overall control breakdown of the system. The Department reported that there is existing policy and guidance information that specifically address the

standards and reporting mechanisms for managing security incidents. The Computer Security Incident Response Capability periodically reports to the CIO on performance measures related to the incidents and information sharing in common vulnerabilities that may affect the Department an/or component agencies. The CIO reported 13 agency components with 12 having incident handling and response capability. Of these components, one reports to FedCIRC.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The Department has 82 reportable systems of which 36 were newly identified systems. The Department reported that there had not been sufficient time to conduct reviews for the newly identified systems. Consequently, the reported information is based on the existing 46 systems. Overall, 98% of the systems, according to the Department, have been assessed for risk with 96% having an up-to-date security plan. Based on the IG's evaluation, of the 16 systems reviewed, 11 had up-to-date security plans (69% compliance.) Nearly all systems had been assessed for risk. The IG indicated that 16 of the 16 systems reviewed in FY 2002 were operating without written authorization.

2. Department methods to ensure contractor services are secure.
The IG reported that they reviewed two of the contractor operations or facilities in FY 2002. In addition, the IG established rules of engagements and performed the related vulnerability assessment testing of a third-party contractor responsible for hosting the Department's financial system of record. The CIO and the Office of the Chief Financial Officer (OCFO) required that the same third-party contractor complete a security self-assessment of the target system. According to the Department, all external service organizations, including contracted services, must provide written certification that they meet the Department's security requirements. The Department reported utilization of three contractor operations or facilities and all three were reviewed by appropriate Department program officials in FY 2002.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that the Department's POA&M process is being effectively implemented and is resulting in a comprehensive approach to identifying system security weaknesses resulting from IG audits. The IG also stated that "there are differences between the POA&M reporting process and IG's audit reporting, tracking, and resolution process, and it is an issue that will be addressed in a timely manner prior to the next target date for reporting progress and improvements to the Department's and component programs' security programs."

The Department reported that the CIO developed and implemented a Department-wide security program based on policy documents and the Department Computer Security Handbook. These requirements were developed using information from the NIST and

commercial industry. The Office of the CIO issues templates for system contingency plans, system security plans, risk assessments, and a Departmental certification and accreditation process to be used for each system. Oversight of security programs is based on the Department's self-assessment process that utilizes NIST methodology and funding resources to conduct detailed reviews of the assessments to assure their validity. The CIO performance measures indicated that 13 components have received security reviews, which related to 100% compliance. Of the 30,963 employees and contractors reported, 93% received security training during FY 2002. This is a significant improvement over FY 2001 where a reported 27% of the agency employees received security training. Of the 673 employees considered as having significant security responsibilities, only 45% received specialized security training. Training costs for FY 2002 indicated a 10% increase over FY 2001 expenses.

2. CIO methods to ensure contractor services are secure.
The IG, in cooperation with the CIO and component program officials, established rules of engagement to perform vulnerability assessment testing of a third-party contractor. The IG also audited another third-party contractor concerning general controls and security audits as part of auditing financial-related systems. The IG reported that they reviewed two of the three Agency managed contractor facilities.

The Department requires its contractors to comply with requisite information security laws, policies, and guidance. All external service organizations, including contracted services, must provide written certification that they meet Department security requirements. The Department periodically assesses contractor compliance using the Agency self-assessment methodology and through inspections. The CIO reported that there were no CIO managed contractor facilities.

3. Agency integration of security and capital planning.
The IG reported that component programs' security requirements and associated cost information are captured in the Department's CPIC process. This information is made available to management for decisions with respect to a component program's state business case.

The CIO integrated security into the Department's capital planning and investment control process. The Office of the CIO reviews each budget request to determine the validity and ensure synchronization with enterprise-wide initiatives. The CIO and Deputy CIO review all Department and component agency IT budget requests to ensure overall compliance with the Department's E-Government Strategy, and the IT strategic plan. FY 2003 capital asset plans and justifications submitted to OMB totaled 30 with all 30 being independently validated prior to submittal to OMB. FY 2004 budget materials indicate 55 submitted capital asset plans and justifications with all being independently evaluated by the CIO or other appropriate personnel.

Department of Transportation (DOT)

A. General Overview

1. Security funding.
The Department of Transportation reports planned FY 2003 funding for IT security of $104M. This funding level comprises 3.8% of their total planned IT portfolio of $2.7B.

2. Number of programs reviewed.
DOT observed the need to clearly identify and define a system inventory methodology that would allow for more consistent reporting. This lead to a clearer understanding of the difference between a "program" and a "system." Thus, more accurate information could be reported by the Department. The Department reported a total of 15 programs with 677 systems. Fifteen programs and 106 systems were reviewed in FY 2002. The Department acknowledges gaps in the inventory process and the CIO developed a template that will be used to build a standardized inventory guide for all DOT Operating Administrations (OAs). The IG also noted that operating divisions used inconsistent methodologies to inventory systems and recommends that the Department develop an accurate systems inventory to identify mission-critical systems for resource allocations, estimate security funding requirements, and to develop performance measures to have its systems assessed, tested, and secured.

All of the OAs used the NIST self-assessment guide to review the mission critical systems and identify weaknesses. The IG reviewed 15 systems and found that they were evaluated based on the self-assessment guide.

3. Material weaknesses.
The IG recognized that the Department implemented a performance measurement program and issued guidance as planned; however, they recommend planned corrective actions for overseeing implementation of security guidance by operating divisions, and securing infrastructure-critical air traffic control systems and assets. The IG questioned the established goal of the Department to have all of its mission-critical systems certified by December 2005 as the projected plan does not indicate that the certifications will be completed within that time frame. The Department advised that material weaknesses had not been reported as required by GISRA Section 3534(c)(1)-(2). DOT reported weaknesses to the Department's policies, procedures, or practices that are required under existing federal guidelines. The Department projected 74 FY 2002 weaknesses with none considered as recurring. FY 2001 performance measures reflect 210 reported weaknesses with none recurring.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The Department had not had a CIO since January 2001 and the Secretary had delegated the Acting CIO the authority to administer GISRA requirements. Full implementation of GISRA

was committed to by the Department and senior leaders in FY 2002. Several cross-cutting improvements within the Department's IT Security Program have been realized with the CIO responsible for identifying and approving all cross-cutting initiatives. A capital planning and investment control policy was issued in FY 2002 which stated the roles and responsibilities of Department and OA leadership referencing IT investment decisions. Operating divisions can make IT investment decisions without review and concurrence by the Office of the CIO.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG is concerned that the Department's performance measures apply only to mission-critical (major) systems and not all Department systems, as required by OMB. Attaining 100% compliance of certification and accreditation will be difficult as the Department had only 22% of the mission-critical systems approved as of September 2002. The Department reported that they have made enhancements to the IT Security Program, based on the findings of the FY 2001 GISRA report. These enhancements include: the development and initial implementation of an IT capital planning process, the use of IT working groups, increased security training, the execution of system audits, the review of proposed software security systems, and annual control reviews to ensure adherence to security requirements. OAs assessed the status of their system security life cycles and are placing increased priority on developing and enhancing IT security plans. The Department implemented the capability to track the OA's completion progress of weaknesses identified in their respective POA&Ms from the FY 2002 GISRA Report. Results of the OA's progress of correcting the deficiencies in the IT security arena are reported to the Secretary and the Leadership Team on a quarterly basis. IT security budgets are also being reported but not monitored to assure adequate financial resources are allocated to IT security.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The IG expressed serious concern over the fact that the FAA had not fully integrated the IT security program with its critical infrastructure protection responsibility concerning physical security at air traffic control facilities. The IG reported in FY 2001 that the FAA did not plan to eliminate physical vulnerabilities until FY 2006. According to the Department, this has now been delayed until FY 2009. The IG strongly recommends that FAA reconsider this schedule to eliminate these vulnerabilities and that the CIO includes a corrective action plan concerning this in its FY 2003 submission.

DOT established the National Infrastructure Security Council (NISC) whose major duty is to rapidly identify and resolve IT security issues affecting the transportation sector. The NISC established an identification and authentication process for governmental and private industry transportation workers. In addition, the Council is collaborating to design logical/physical common access architecture, using smart card technology, to resolve identification and authentication, and logical/physical access control issues. Seventy-three percent of OAs developed and updated Continuity of Operation Plans (COOP), which will improve the overall IT security structure by integrating plans for recovering business operations in the event of a loss of mission critical physical and/or logical assets. The CIO required all OAs to submit the updated COOP and Continuity of Government (COG) plans for review.

4. Critical asset prioritization and protection methodologies.
The IG reported that, because the Department failed to fully evaluate the system interdependencies in the informal evaluation process, two additional air traffic control systems were not considered as critical assets in the FY 2001 report. These two systems have been added per the findings of the IG. The IG also reported that the Department was in the early stages of data collection and had not yet developed a work plan detailing the tasks, milestones, or funding commitments of the Department. As reported in FY 2001, the Department did not use any specific methodology in identifying its critical assets. The Department initiated the implementation of Project Matrix in its effort to identify critical operations and assets. The discovery phase of Project Matrix was initiated in the third quarter of FY 2002. Data collection of critical systems and assets is currently being conducted and the CIO will continue to work with the OAs to continue to properly identify mission-critical systems and to adjust the inventory as necessary.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG determined that the interim reporting guidelines were not effectively implemented and needed to be improved. The IG acknowledged that the Department reported more than 25,000 incidents to FedCIRC during FY 2002; however, they are concerned that the Department did not analyze whether these incidents were caused by intrusion activities or by innocent acts such as typing the wrong password. The IG cautions that while DOT was reporting innocent acts to agencies outside the Department, significant incidents were not reported as required.

The Department states that they made significant improvements in their Incident Reporting and Handling process in FY 2002. The Department reported 57,710 incidents internally and 25,595 incidents were reported to FedCIRC or law enforcement. The CIO developed and executed an Incident Reporting Policy Memorandum and began reporting incidents on a weekly basis. The Department continued to implement intrusion detection systems at critical access points throughout the DOT backbone. There are reported gaps in implementing consistent incident detection and reporting capabilities. The Department advises that they must concentrate more on participating in the FedCIRC patch management system and also expand intrusion detection system coverage and reporting to a larger percentage of DOT IT systems.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reported that the Department decided to first focus on getting mission-critical systems assessed and tested. Operating divisions had not yet assessed risk, determined the appropriate security level, updated the security plan, and tested the security controls for each system under their control. The Department had not developed a schedule to have the remaining mission-critical systems assessed. The IG also found that the Department needs to

establish a complete and accurate systems inventory and to develop an adequate plan to access the non-mission critical systems.

The Department indicated that all of the DOT OAs have developed and/or completed both risk and security assessments for a portion of the operations and assets under their control. Twenty-two percent of the security systems had been certified and accredited, a 12% increase over FY 2001. The Department agreed that improvement in certification and accreditation and instituting a consistent inventory methodology and schedule is paramount in FY 2003.

2. Department methods to ensure contractor services are secure.
The IG's review of outstanding contracts revealed that only one independent review was required by the Department out of four data center operations and 35 web system operation contracts. The IG also reported that one web system contracted to a third party was defaced. The IG noted that although the Department had issued additional guidance concerning unsecured network connections, the guidance had not been implemented. This was evidenced by the IG's discovery of three unsecured contractor connections at one FAA site. The IG recommended that the Department continue to improve background security checks as there is a lack of overall compliance with this Department policy.

The Department developed draft guidelines for ensuring the security of supporting services as provided by outside contractors. The Department worked with senior Department security and procurement officials to develop a detailed clause for use in IT support service contracts requiring contractors to follow more stringent government security requirements and background investigation policies.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The Department issued specific guidance addressing network security, incident reporting, and capital planning. The IG is concerned that this guidance is not being effectively implemented by the operating divisions. The IG contends that the CIO lacks direct supervision of security program implementation and guidance due to a lack of budget or performance authority over operating divisions.

According to the CIO, each OA is evaluated monthly on their performance. Additionally, the Department increased the development and oversight of Department-wide security programs by hiring an Associate CIO for Security. This position provided the Department with increased oversight to ensure that security programs and IT security performance are effectively implemented by the OAs. The Department contends it maintains a successful security program as indicated by the improvements evidenced in the performance measurement program. All OAs reported having at least a limited security program in place. Training costs exceeded $900K in FY 2002 with 105,000 employees and contractors and 999 employees with significant security responsibilities receiving additional security training.

2. CIO methods to ensure contractor services are secure.

The IG's review indicated that security background investigations were not being conducted as required pursuant to Departmental policy. The CIO advised that all contractors must meet the requirements of NIST SP 800-26 security control requirements and must currently have appropriate background investigations per Departmental policy.

3. Agency integration of security and capital planning.
The IG reported that, although the CIO made a concerted effort to develop its IT capital planning and investment control process, OAs did not fully implement this guidance. Further training on the estimation of security costs and the development of a matrix in the E-GOV scorecard to measure OAs compliance will be provided by the Department in FY 2003. For FY 2003, 25 major system and 117 general support system capital asset plans and justifications were submitted to OMB. For the FY 2004 Budget Materials, 86 major application and 330 general support system business cases were submitted to OMB. The Department will complete IT security integration with Enterprise Architecture and will incorporate process improvements into the CPIC based on lessons learned in the FY 2004 budget process to include establishing and enforcing processes for estimating security costs within all investments. The goal of the Department's CPIC process is to make information resource investments that improve mission effectiveness, efficiency, and information security. Costs, resources, and schedules to implement security safeguards defined in the Security Plan should be developed and incorporated in the business case. When business cases are reviewed and prioritized collectively with other candidate project initiatives for inclusion in budget requests, IT security factors will be a critical criteria in the decision-making process.

Department of the Treasury

A. General Overview

1. Security funding.
The Department reports planned FY 2003 funding for IT security and critical infrastructure protection of $80.5M. This funding level comprises 3% of their total planned IT portfolio of $2.56B.

2. Number of programs reviewed.
The IG is responsible for evaluating Treasury's components, except IRS. The Treasury Inspector General for Tax Administration (TIGTA) is responsible for assessing IRS programs. The IG and TIGTA evaluated the components' program system self-assessment methodologies used in FY 2002. Each compared the elements of the Treasury Self-Assessment Framework (TSAF) with OMB's required use of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology Systems. Their analyses showed that TSAF did not address, in detail, the critical elements outlined in the NIST guide and that a review performed using TSAF would not result in the same determination as to the current security

status of a component's information system. Treasury will require the use of the NIST guide in conducting FY 2003 self-assessments.

The IG reported that Treasury has 51 programs supported by 626 systems. The number of agency programs in FY 2002 increased (39 in FY 2001 to 51 in FY 2002) because Treasury provided specific definition for agency "programs" to avoid misinterpretations at the component level. Treasury also reported a total of 51 programs in FY 2002, but its numbers from this point on do not agree with what the IG has reported. Treasury indicated 48 of the 51 programs were reviewed.

In FY 2002, Treasury reported that 451 of its 624 systems were reviewed while the IG reported 204 of 626 systems were reviewed. Of the 451 systems, Treasury indicated that 352 systems were reviewed using the NIST guide (IG reported that 41 systems were reviewed using the NIST guide. Treasury reported that 71 systems were reviewed using the Treasury methodology, addressing all 17 of the critical elements found in the NIST guide, while the IG indicated that 163 assessments were conducted using methodology other than the NIST guide.

3. Material weaknesses.
In FY 2002, a total of eleven material weaknesses were reported, including 9 repeated from FY 2001. The US Mint reported two new material weaknesses in FY 2002. The Department's weaknesses included issues such as sensitive systems lacking certification and accreditation, timely restoration of mission-critical systems, inappropriate access to programs/data files, and ineffective computer controls in some of the bureaus, including lack of policy guidance and oversight of these controls.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The Secretary, the Treasury Chief Information Officer (CIO), and component CIOs took steps in FY 2002 to set forth GISRA responsibilities and authorities. An August 2002 memorandum from the Assistant Secretary for Management and Chief Financial Officer stipulated that each component head is required to oversee the performance of all component program officials and the CIOs to verify that IT security plans are up-to-date and practiced throughout the program life cycle. In addition, IT security is to be considered an essential management concern; capital asset plans will fully address all IT security requirements and costs; all IT systems and major applications are to be properly certified and accredited for operation; and all employees, including contractors, will receive IT security training. Furthermore, a major operating component of Treasury cannot make an IT investment decision without a review by and concurrence of the Treasury Investment Review Board (IRB). In addition, to ensure that Treasury Bureaus comply with GISRA requirements, the Treasury CIO is initiating an IV&V process in FY 2003 with the objective of ensuring an adequate level of compliance assurance and accuracy of Bureau reporting.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported that Treasury made progress to ensure proper oversight of the performance of program officials and component CIOs but two issues surfaced in the IG review. (1) The Office of Compliance and Oversight was only able to perform limited reviews for 21 system security plans at four of Treasury's 16 components. (2) The IG found that security plans had not been completed for 391 (62 percent) of Treasury's 626 systems.

Treasury indicated that its Office of Information Systems Security (OISS) conducted 35 security reviews of Bureaus' information systems and programs to ensure that security programs and plans are current and practiced throughout the life cycle of each information system. Nineteen Bureau Compliance Program Oversight visits were conducted which included personnel interviews, security document validation, Security Training and Awareness Program assistance, and Security Oversight methodology guidance. Fourteen security documentation reviews (system security plans and system security authorization agreements) of critical CIP systems that included corrective action and/or response by the subject Bureau were completed. Two program reviews of the Department's and the Treasury CIO's information systems also were done. The OISS conducted a review of the Treasury Security Incident Response Reporting System and facilitated the review of the Departmental Offices (DO) Electronic Mail System by the National Security Agency.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG reported that Treasury made progress in strengthening its critical infrastructure program. The Department now has a Treasury Critical Infrastructure Protection Plan (TCIPP) that provides guidelines to components for integrating its IT security programs and for critical infrastructure protection responsibilities. Each component shares responsibility for identifying the critical assets under its cognizance, assessing the vulnerabilities of those assets, and assuring their availability, integrity, confidentiality, survivability, and adequacy.

Although progress was made for critical infrastructure protection, the IG identified areas in which Treasury needs to improve. As indicated in their FY 2001 review, the IG reported that both funding and human resources impacted Treasury's critical infrastructure program. Both the physical and cyber components of the Critical Infrastructure Protection Program (CIPP) were consolidated.

Treasury's Critical Infrastructure Assurance Officer (CIAO) oversees the planning, development, and implementation of critical protection/assurance requirements Treasury-wide. The CIAO established the Critical Infrastructure Protection (CIP) Working Group to facilitate department-wide collection, management, and dissemination of CIP-related materials, direction and guidance. In addition, each component was required to identify a CIP Officer (CIPO) who is responsible for integrating and coordinating CIP requirements within and among the components' various security programs and infrastructure asset owners.

4. Critical asset prioritization and protection methodologies.

During their FY 2002 evaluation, the IG found that although funding was originally identified for Project Matrix (PM) in FY 2002, the funding was diverted to other Departmental programs. In addition, at the time of the review, funding was not set-aside for a Project Matrix review in FY 2003.

In April 2002, Treasury hired an independent contractor to assist in performing required interdependency analyses. Treasury created its own methodology for conducting interdependency analysis because the national CIAO methodology was too general and did not address Treasury's specific needs. In addition, TIGTA reported that the IRS had not undergone a Project Matrix review, but identified its critical operations and assets.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG reported that Treasury made some progress in complying with the standards set by OMB and GISRA to establish and implement an agency-wide Computer Security Incidents Response Center (CSIRC). On August 1, 2002, Treasury established and implemented a 24-hour CSIRC. As reported in the IG's FY 2001 review, Treasury's CSIRC policy and incident response procedures had not been formally approved. The Department anticipated formally issuing its CSIRC policy and incident response procedures during FY 2003.

IG findings indicated that Treasury's CSIRC officials had not reviewed the integrity of security incidents that were reported. It appeared that computer incidents and reporting requirements are viewed differently among component officials. The Department had not enforced its CSIRC procedures to ensure that components comply with a consistent methodology to identify, document and report computer security incidents.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
Treasury established a performance measure to track the percentage of IT systems that are certified and accredited. Although an 18 percent improvement over last year was reported, the majority of the Department's systems were not certified and accredited in FY 2002.

2. Department methods to ensure contractor services are secure.
The IG indicated that Treasury had not demonstrated progress in implementing appropriate methods to ensure that contractor provided services are adequately secure. While the Department drafted a security program policy that includes the requirement that program officials ensure that contractor provided services are secure, the policy had not yet been implemented. Nevertheless, six of the 16 (38 percent) components developed their own security policies to ensure services provided by contractors and external agencies are secure. In FY 2002, program officials at five of the 16 (31 percent) components conducted contractor service reviews and inspections to ensure contractors met security guidelines and requirements.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
According to the IG, the number of employees that received annual security awareness training decreased from 85 percent in FY 2001 to 72 percent in FY 2002. The IG reported that this decline is largely due to component's inability to support training numbers.

According to the IG's report, Treasury established a Department-wide security program responsible for the planning, implementing and managing security policy, cyber critical infrastructure protection, and oversight and compliance. Additionally, the IG reported, 15 of 16 components offered specialized training to employees with significant information systems security responsibilities with 79% of those employees receiving specialized training as of August 2002.

2. CIO methods to ensure contractor services are secure.
Treasury drafted a Security Program Policy that provides baseline security guidance for its components, including DO, OIG, and TIGTA. The IG review of the draft policy found that it did not address contractor provided services or assessments of contractor provided services. Therefore, appropriate methods had not been used to ensure contractor provided services or services provided by another agency are adequately secure. (See also C.2.)

3. Agency integration of security and capital planning.
The IG reported that Treasury made progress in addressing this area in FY 2002. Based upon its overall analyses and verification, the IG found that security requirements and costs were reported in the FY 2003 capital asset plans (as well as in the Exhibit 53s) that Treasury submitted to OMB. Additionally, security information and costs were being documented in the draft FY 2004 capital asset plans. However, two areas of concern were identified: (1) the IG was unable to validate whether capital asset plans had been prepared for each of Treasury's major systems. (The IG notes that individual components determine whether systems are major, i.e., needing a capital asset plan) (2) The methodology needed to justify IT security costs for investments is not documented in the security information included in components' capital asset plans. Therefore, reported security costs cannot be independently verified or validated if the methodology used to calculate the amounts is not documented.

Environmental Protection Agency (EPA)

A. General Overview

1. Security funding.
The Agency reports planned FY 2003 funding for IT security of $8M. This funding level comprises 1.9% of their total planned IT portfolio of $432M.

2. Number of programs reviewed.
The Agency consists of 10 regional offices, 13 program offices and the Agency's central infrastructure for a total of 24 Agency programs. The Agency reported that all programs

were reviewed in FY 2002 and 168 systems within the 24 programs were reviewed. The IG was not able to confirm the system reviews as their independent evaluation was completed on July 30, 2002. The IG did advise that the Agency planned to finalize the actual list by the end of August 2002.

FY 2001 GISRA report evidenced the review of 189 systems. The FY 2002 report reflects the completion of 168 system reviews and states that the reduction of reviews from FY 2001 is due to system retirement, consolidation and reclassification.

The NIST Self-Assessment guide was used for the FY 2002 security system assessments.

3. Material weaknesses.
The Agency closed out its FY 2001 reported material weakness in Information Systems Security. There were no additional material weaknesses reported in FY 2002 and the IG recommended that the Information Systems Security material weakness be downgraded to an agency-level weakness. The IG based this recommendation on their observation of the Agency's "considerable" progress made in implementing its computer security program.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG review of Agency IT investments indicated that approved investment proposals submitted to OMB in November 2001 were the same ones approved by the CIO in the September 2001 advisement memorandum. The IG advised that additional improvements can be made to the Agency's capital planning and IT procurement processes and will issue findings in a later report. The CIO was formally delegated GISRA responsibilities by the Agency head, and as such, is responsible for ensuring that the requirements of GISRA are implemented and communicated. The Agency also executed legal documents granting authorities of the Administrator to senior Agency managers or representatives, making the delegated person fully responsible and accountable for actions taken in exercising the delegated authority. The CIO used several venues to ensure effective implementation of GISRA by – providing senior Agency program officials with a quarterly IT security scorecard, providing a quarterly analysis of computer security incident trends that should be used to enhance IT security practices, and annually evaluates major IT investments for compliance with the Agency's policy on capital planning and investment control. Provided the Agency strictly adheres to this policy, no major IT investment decisions can be made without review and concurrence by the Agency's CIO.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported that the Agency had not developed a dedicated process for ensuring that security plans of general support systems and major applications are up-to-date and practiced throughout the life cycle of each system. CPIC reviews are limited to major systems or applications that contain data defined as having a "high" sensitivity level. The IG stated that "at this time, the Agency does not verify the existence of security plans for those systems and

applications that do not fall into these categories." The Agency head delegated the CIO the responsibility of establishing and maintaining a continuing program for the management and security of records, files, data, and information systems and technology. The CIO reported that several actions were initiated to oversee the performance of program officials in maintaining up-to-date security plans practiced throughout the life cycle of each system. The CIO also reported that the Agency is updating it System Live Cycle Management policy to more clearly articulate information security requirements at all stages of a system's life cycle. This is confirmed by the IG who indicated that the Agency's current Life Cycle Management policy is "outdated". The Agency's FY 2001 GISRA report indicated that such policies would be updated; however, they still have not been completed.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The Agency's Critical Infrastructure Protection Plan (CIPP) was developed in collaboration with several Agency offices that have different responsibilities for critical infrastructure protection. The responsibilities for assessing and addressing vulnerabilities are aligned with each office's overall mission. Within the Agency, these overall infrastructure assurance responsibilities are shared by the Office of Administration of Resource Management (OARM), the Office of Solid Waste and Emergency Response (OWER), and the Office of Water (OW). OARM maintains responsibility for the Agency's physical and cyber infrastructure protection functions, OWER has emergency and remedial response obligations, and OW is responsible for developing a water supply sector Critical Infrastructure Assurance Plan. The CIO reported that the Agency continues to protect its critical IT infrastructures through implementation of policies, procedures and standards developed through the Agency's IT security program, conducting risk assessments to identify weaknesses, implementing or improving security controls, and developing POA&Ms for mitigating weaknesses and tracking progress in completing milestones. The Agency developed a continuity of operations plan as well as a disaster recovery plan for the National Computer Center (NCC) which they consider a component of the Agency's critical infrastructure.

Separate staffs are devoted to other security programs and these programs are under the authority of different Agency officials. The IG reported that there is no apparent duplication of effort with the responsibilities of these programs. The IG did report that one responsibility is shared by two offices, but they consider this as a shared responsibility rather than a duplication of effort.

4. Critical asset prioritization and protection methodologies.

The Agency concluded step one of the three-step Project Matrix process. A draft report had been developed that identified the Agency's critical assets. Prior to the report being finalized, the IG reported that it must undergo a quality assurance process to ensure that senior Agency officials agree with the findings. The IG recommended that once the report is finalized, the Agency needs to complete a vulnerability assessment and risk mitigation plan for all of its cyber-based assets.

5. Department documented procedures for reporting and sharing vulnerabilities.

The IG advised that the Agency, through the Office of Environmental Information (OEI), has decided to out-source the Incident Handling Program function. According to the Agency, all 24 bureaus have incident handling and response capabilities. The Agency centralized incident report processing and established a Computer Security Incident Response Center (CSIRC). Security incident reports are maintained in a secure part of a central Agency database, REMEDY. All incidents are also reported to the Cyber Crimes Unit (CCU). CCU, as part of the Office of the IG, has direct access to REMEDY to assure they are kept up-to-date on IT security incident activity. Weekly incident reports are summarized by the Agency's Technical Information Security Staff (TISS) and submitted to FedCIRC. The Agency began providing FedCIRC with the incident data in September 2001. Of the reported 572 Agency incidents, 311 were reported to FedCIRC in FY 2002. The number of incidents reported by the Agency is lower for FY 2002 than FY 2001 (1,430) because of a change in how the Agency is tracking incidents. The Agency concluded that the FY 2001 numbers were not reliable as the incidents reported were based on the number of incidents self-reported by each program and office, independently of whether they were reported to REMEDY.

The CIO does not report IT security incidents to external law enforcement. Rather, incidents with criminal ramifications are reported to the IG's Computer Crimes Directorate (CCD). The CCD then reports such incidents to the proper law enforcement authorities as they deem appropriate.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.

The Agency reported that they have a total of 168 major applications and general support systems and that all of these applications and systems were assessed in FY 2002 using the NIST Self-Assessment Guide. The IG reported that only 80% of program offices had completed risk assessments for all assets and operations under their control. The 20% difference, according to the IG, represents assets and systems that the Agency did not label as "major applications" or "general support systems" for GISRA reporting purposes. These applications operate on the Agency's network and pose inherent security risks. The IG recommends that they undergo risk evaluation, whether conducted by the OEI or the responsible program office.

Only 18% were operating with tested contingency plans. An IG review of key data elements in the Agency security plans indicated that a significant number of security plans were not comprehensively addressed to meet the standards set forth in NIST Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems." Noted areas that were not addressed include: risk assessment methodology used to identify threats and vulnerabilities; security activities required for its current phase; and contingency plan procedures. The IG suggested that the problem occurred because the Agency's security plan guidance predated revisions to NIST guidance and OMB A-130, Appendix III, which describe and organize basic security plan requirements. The Agency indicated that compliance with security planning requirements has improved but noted that more effort is

necessary in ensuring that all system security plans are approved by key affected parties and management, i.e., authorized for operation. The Agency also identified that improvements are needed in the contingency planning area and that substantial attention is required to strengthen the Agency's overall testing and evaluation practices. The Agency reported that it is working with the responsible program official to develop POA&Ms to correct these deficiencies.

2. Department methods to ensure contractor services are secure.
The IG reported that, as of July 22, 2002, only one program had performed reviews or inspections by Agency program officials to ensure that contractor-provided services or services provided by another agency for their program and systems were adequately secure and met regulatory requirements. The Agency reported that 32 of the 50 contractor operations or facilities had been reviewed using methodologies that include physical inspections, document reviews, software testing, and assessments based on NIST 800-26.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that while the Agency had more work to do in this key area, they did issue or update several security-related policies and procedures and plan to complete additional ones in FY 2003. The IG noted that all of the security-related policies and procedures identified as completed in FY 2002 existed and, in fact, were issued or updated as management had indicted. The IG also noted that OEI is beginning to establish some security oversight for the Agency's complex IT network; however, the IG recommended that the Agency focus more on independent verification, validation, and enforcement of the implementation of its security program. The Agency maintained that their IT security program is managed by the security staff under the Deputy CIO for Technology, overseeing the development, maintenance and implementation of the Agency-wide security program which consists of planning and policy, implementation of controls, training and communication, and evaluation.

The CIO reported that 100% of the Agency components and field activities had security reviews. IT security training was provided to 37% of Agency employees and contractors. While this percentage is significantly less than in FY 2001 where 93% of employees and contractors received training, the difference is a result of the Agency changing its security awareness training cycle from a fiscal year to calendar year basis. Total training costs increased from $798K in FY 2001 to $1.4M in FY 2002. The IG suggested that to establish a robust and effective IT security training program, the Agency should identify personnel with significant security responsibilities and assess security training needs for those personnel.

2. CIO methods to ensure contractor services are secure.
The IG found that the Agency's actions for ensuring contractor services comply with GISRA. The IG did recommend that the Agency work to finalize penetration testing to establish identified weaknesses and to establish POA&Ms for such weaknesses. Additionally, the IG recommended that the Agency develop and implement strategies to address concerns regarding oversight reviews of the IT systems network. In particular, the CIO has

responsibility for a variety of contract services which support the Agency's IT enterprise network operations, network security, and systems development activities. The CIO conducted risk assessments on the National Computer Center (NCC), the Headquarters LAN, the TRI Reporting Center, and the Central Data Exchange (CDX).

3. Agency integration of security and capital planning.
Although the Agency reported that they integrated IT security into its capital planning and investment control process, the IG reported that full integration of security has not occurred. While significant improvements have been attained, weaknesses remain in the areas of policy guidance, quality assurance, and systems inventory. The Agency reported that 48 capital asset plans and justifications were submitted to OMB in the FY 2003 budget materials and 39 have been submitted in the FY 2004 budget material.

Federal Emergency Management Agency (FEMA)

A. General Overview

1. Security funding.
The Agency reports planned FY 2003 funding for IT security and critical infrastructure protection of $8.8M. This funding level comprises 1.5% of their total planned IT portfolio of $582M.

2. Number of programs reviewed.
The IG reported that FEMA did not have a methodology for maintaining current inventories of agency mission critical systems. Nor did FEMA have a complete listing of all devices with wireless connectivity capabilities. FEMA confirmed that the lack of a complete inventory of wireless enabled devices elevates the security risk for the agency.

The Agency is comprised of 11 major components that are supported by 51 identified, unclassified general support systems and major applications. During FY 2002, FEMA reported that it reviewed eight of the 51 systems but none of its 11 programs.

3. Material weaknesses.
The IG concurred with FEMA's reporting of material weaknesses. FEMA reported a total of eight repeat material weaknesses from FY 2001 and no additional material weaknesses in FY 2002. These include weaknesses in the overall system security program, security control implementation in individual system life cycles, contingency planning, computer security education and awareness, personnel security, risk assessments, security life cycle management, and certification and accreditation.

During FY 2002, as part of a comprehensive IT management reorganization, FEMA implemented an organizational structure to better facilitate addressing its information security material weaknesses, including establishing and filling the position of Chief Information Security Officer (CISO). The CISO reports directly to the FEMA Chief

Information Officer (CIO). FEMA made progress in addressing these weaknesses but recognizes more needs to be accomplished before these areas can no longer be assessed as material weaknesses.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
FEMA realigned its IT security resources and staff within the FEMA Information Technology Services Directorate (ITSD). This resulted in more efficient and effective communication within the Directorate. In addition, the realignment established the FEMA Office of Cyber Security (OCS) to better support the Agency's business decisions and capital planning initiatives that impact the security program and protect mission critical IT programs and systems. Zero-based budgeting was implemented, requiring all new FEMA programs or projects to go through a review process and earn director-level approval. Also, the FEMA CIO restructured the Agency's Information Review Management Board (IRMB) to implement the FEMA IT capital planning and investment control (CPIC) process. The IRMB serves as the approval authority for investment decisions involving selected projects related to major IT systems. FEMA's Zero-Based Budget and IT CPIC process enforce proper reviews and authorization of new IT initiatives and drive investment decisions.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported and FEMA concurred that although FEMA made progress with several initiatives to further the Agency's IT security program, its current security program did not ensure consistent implementation of security controls in individual system life cycles.

The Agency's FY 2002 implementation of a highly structured IT CPIC now specifically includes a System Development Life Cycle. OCS actively participated in the development of the IT CPIC Guide and implementation to ensure that the NIST-specific security life cycle was incorporated. Using this approach, approval of projects depends on the demonstration of adequate security across the life cycle.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG concurred with FEMA that progress was made in the development of a Certification and Accreditation (C&A) methodology, which includes review elements for several components of agency systems and processes (e.g., physical security, contingency planning, and operational security.) However, the IG noted that FEMA still needs to make substantial progress in implementing the C&A methodology across the agency, as no systems had received a C&A.

FEMA reported it implemented security controls across the majority of its systems, but not consistently across all systems. The NIST Computer Security Expert Assistance Team (CSEAT) recognized that FEMA had established operational controls, including firewalls and an incident response team. The National Security Agency's "Red Team" penetration

testing results and system audits conducted by FEMA contractors support the position that FEMA's systems have security controls implemented for exterior protection. FEMA's goal is to ensure a consistent level of implemented security controls on every system by making use of formal security planning activities. The Agency is taking steps to review security controls of their internal network infrastructure through structured risk assessments. Based on these risk assessments, a consistent set of Baseline Security Controls are specified to address the security of each individual system.

4. Critical asset prioritization and protection methodologies.
Both the IG and the Agency reported that FEMA had not yet fully completed a Project Matrix review. In December 2000, the Agency Information Assurance (IA) Branch reviewed FEMA's IT systems based upon the Critical Infrastructure Assurance Officer's (CIAO's) Infrastructure Asset Evaluation Survey. The IA Branch identified 12 General Support Systems (GSSs) and Major Applications (MAs) mission critical systems based upon their degree of importance to the FEMA mission. In FY 2001, the Agency underwent the discovery phase of a Project Matrix review, but made little progress on it in FY 2002. FEMA anticipates completing this review in FY 2003. In the meantime, with the establishment of the Agency's OCS, an Agency-wide security program is being implemented that complies with OMB, NIST, and other federal requirements. FEMA implemented the IT CPIC and restructured the IRMB to ensure the appropriate review and approvals for new Agency programs and systems.

5. Department documented procedures for reporting and sharing vulnerabilities.
Both the IG and FEMA reported that the Agency has the technical and procedural means in place to detect and report security incidents and share information on common vulnerabilities. FEMA's OCS implemented an incident reporting process and documented it in its Enterprise Security Manual (ESM).

During network vulnerability assessment, the IG tested FEMA's intrusion detection capabilities and noted that improvements had been made since FY 2001. No intrusion incident reports were made by FEMA's OCS during FY 2002 to FedCIRC.

The IG noted that although FEMA maintains the Configuration Control Board (CCB), FEMA's overall process for tracking software patches does not provide for consistent controls to ensure that patches are installed in a timely and effective manner. This control weakness contributed to the identification of security vulnerabilities during the IG IT controls review supporting the FY 2002 financial statement audit. Several of these weaknesses were also identified during the IT controls review supporting the FY 2001 financial statement audit.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
During FY 2002, FEMA engaged a contractor to assist with the development of the Agency's Certification and Accreditation (C&A) methodology. FEMA is using this C&A

methodology in lieu of NIST SP 800-26 to perform agency information security reviews. The IG reviewed the methodology and found that it generally complied with the Federal Information Processing Standards Publication (FIPSPUB) 102, Guideline for Computer Security Certification and Accreditation and relevant NIST guidance. However, FEMA's C&A process, as it is currently operating, has OCS coordinating the completion of the various security documents needed to support a system C&A. OCS has engaged a contractor to assist with developing these documents. In order to ensure segregation of duties within the C&A process, the FIPSPUB guides that agency program officials should be responsible for completing the necessary C&A documentation, and the agency's certifying body (OCS in FEMA's case) should independently validate whether the documentation package is sufficient to justify a C&A.

FEMA indicated that eight of its 51 systems had been assessed for risk; 13 of the 51 systems had an up-to-date security plan; none of the systems had been certified and accredited, therefore, all 51 systems were operating without written authorization. In addition, the Agency reported that only 5 systems had the costs of their security controls integrated into the life cycle of the system; eight systems had their security controls tested and evaluated in the last year and had a contingency plan. However, none of the systems had those contingency plans tested in the past year.

2. Department methods to ensure contractor services are secure.
During FY 2002, as part of FEMA's C&A methodology, risk assessments were initiated and were ongoing for two agency contractor operations. While the IG acknowledged this activity as a positive step, the IG further recommended that FEMA develop a complete inventory of all agency IT service providers and the services they provide, and assess a level of risk to these service providers to ensure that the highest risk providers are reviewed as soon as possible. The IG recommended that FEMA have a process in place to ensure that periodic assessments of information security controls are conducted. In addition, FEMA received IT support from Federal agencies, including the Department of Agriculture and the Department of Health and Human Services, which also should be assessed as part of FEMA's service provider inventory and risk assessment process.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
FEMA's realignment of security resources during FY 2001 and 2002 improved their capability to develop and administer a more effective and efficient Agency-wide IT security program. In particular, during FY 2002, the Agency made great strides to ensure that the security program was focused on compliance with all federal and FEMA security requirements. Both the IG and FEMA are in agreement that Agency needs to develop better general information security awareness training and specific training for information security personnel. To help address this issue OCS developed the Information Security Concept of Operations to identify skill sets needed to accomplish specific tasks for each of the OCS functional areas.

As part of the Agency's information security program, the IG indicated that FEMA needs to ensure that all personnel who have significant information security responsibilities, not just those within OCS, are identified. FEMA must ensure that all personnel are aware of their information security responsibilities and that adequate training is provided to them. In addition, FEMA needs to implement metrics to better track costs and feedback related to information security training.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
During FY 2002, FEMA began implementing corrective actions to improve its IT capital planning. The Agency: 1) revamped the IRB into the IRMB; 2) is attempting to make the IRMB more proactive during the process of selecting investments into the Agency's IT portfolio; and 3) is revising its *Capital Planning and Investment Control Guide* to provide more explicit IT capital planning guidance to agency system managers. These improvements will need to be linked to FEMA's overall IT organization processes, including the Agency's information security program.

General Services Administration (GSA)

A. General Overview

1. Security funding.
The General Services Administration reports planned FY 2003 funding for IT security of $25.2M. This funding level comprises 5% of their total planned IT portfolio of $513M.

2. Number of programs reviewed.
The Agency identified 56 total systems and reviewed 23 systems using the NIST Self-Assessment guidelines. Two systems were reclassified in July 2002 and were not reviewed using the NIST questionnaire for FY02 due to limited time constraints. The IG obtained information from six select IT systems across the Agency's Service/Staff Offices and also used the NIST process for their evaluations.

3. Material weaknesses.
Both the IG and the agency reported that there were no material weaknesses identified during FY 2001 and FY 2002. However, the IG did identify two reportable conditions based on financial statement audit results. The conditions noted are: (1) entity-wide system security management and oversight continue to need improvement, and (2) development, implementation, and change controls over the Agency's system environment continue to need improvement.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG reported that the Security Division has published 15 IT security procedural guides on topics such as conducting risk assessments, password generation and protection, incident handling, security testing and evaluation, and developing a configuration management plan. The Security Division developed a compliance review schedule for Services/Staff Offices and Regional security controls, performed annual Security Act evaluations, and developed an agency-wide POA&M. Other areas of controls were initiated by the Security Division, including, agency-wide external penetration testing, development of a standard software image that contains security controls, development and distribution of IT rules of behavior, and development of a draft policy for the use of wireless LANs.

The Agency reported that the Administrator is committed to and is appropriately involved in the management of risk across the Agency. The CIO and program officials' responsibilities for GISRA requirements had been clearly set forth by the Administrator. The Agency designated a Senior Agency Security Official who serves as the focal point for central security management. In addition, the Agency established the Security Division in the Office of the CIO, whose responsibility it is to address planning, development, implementation, maintenance and enforcement of the IT Security Program for the Agency. The Agency CIO is involved in the review of all IT investment decisions.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Agency developed performance measures, which are reviewed by the Administrator on a quarterly basis. Specific performance measures include: percent deviation of GISRA weaknesses mitigated; percent of high risk vulnerabilities resolved within 30 days; percent of Agency associates completing annual security awareness training; and percent of major IT investment projects within planned cost goals. The Agency's annual GISRA evaluation is also used by the Agency's Administrator to determine if up-to-date risk assessments, security plans, system testing and evaluations, and certification and accreditation packages have been completed for Agency systems.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG reported that PBS and FSS had established Service level IT security policy and procedures, and FTS drafted IT Security policy, to manage their systems. The IG found that these Service level IT security policies and procedures generally support the Agency's IT Security Policy. The Agency took several steps to integrate IT security with its critical infrastructure protection program. This includes assigning the Critical Infrastructure Assurance Officer (CIAO) duties immediate to the CIO, appointing the CIO as the CIAO during FY 2002, and establishing an internal organizational structure for the Office of the CIO that includes critical infrastructure responsibilities within the Security Division. The Security Division published security guidelines as noted above which assists in infrastructure protection.

4. Critical asset prioritization and protection methodologies.

In FY 2001, the Agency began a Project Matrix review. In order to identify the Agency's assets that may be potentially critical to national infrastructure assurance, the CIAO was provided with a list of approximately 128 assets that the Agency relies on for its day-to-day operation. At the completion of Phase One of the Project Matrix review, the CIAO reported that three assets were found to be nationally critical assets. Phase Two was scheduled to be completed during FY 2002 and Phase Three was scheduled to be completed during FY 2003.

5. Department documented procedures for reporting and sharing vulnerabilities.
The Agency's Security Division implemented a framework for incident reporting, incident response, and information sharing that integrates the efforts of all Agency Services and Staff Offices. Law enforcement and/or FedCIRC are notified if an incident is deemed "significant" pursuant to the Agency's IT Security Policy. All external incidents are reported to FedCIRC, all issues requiring law enforcement are reported to the IG, and internal incidents are addressed initially through internal management. The Agency has three components that have incident handling and response capability and one component that reports to FedCIRC. The Agency S/SOs are required to report incidents within 24 – 48 hours of the occurrence. The Agency undertook a number of activities to improve reporting and protection against vulnerabilities, such as Security Division guidance, proactive network and Internet vulnerability scanning, increased IT security awareness', C&A activities, and centralized firewall change request coordination through the Security Division. The IG reported that requirements of the Agency's IT Security Policy and IT Incident Handling Guide for reporting to law enforcement authorities and FedCIRC are "general in nature and do not include instructions for reporting to the IG."

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reviewed six select IT systems for security controls. The IG concluded that while the status of security controls of select systems reviewed last year had not significantly improved, the results of their review for FY 2002 sample of systems generally found a higher level of security controls in place.

The Agency reported that all 56 major application and general support systems were reviewed for security controls and that 23 major application and general support systems received detailed reviews using the NIST 800-26, "Self-Assessment Guide for Information Technology Systems." The Agency also reported improvements in the number of current security documents addressing risk assessments, security plans and testing and evaluation. Additionally, the Agency identified an increase in the number of contingency plans developed in FY 2002.

2. Department methods to ensure contractor services are secure.
The IG reported that the Agency's compliance monitoring of contractors' or external agencies' security has been limited to reviewing physical security controls at select contractor operated data centers. Additionally, the IG reported that for the six systems they reviewed in FY 2002, they were unable to locate system specific security procedures within

contractors' Statements of Work. The IG commented that, while the Agency compiles data related to physical security reviews of contractor facilities, they do not actually perform the evaluations. Contractors are responsible for complying with the Agency's IT Security Policy and guidance, general IT security practices, and procedures specific to the systems. The Agency reported that of the 42 contractor operations across the Agency, 27 had completed reviews in FY 2002.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.

The Agency, working through the Security Division, has a framework for information security that is based on the development, maintenance, implementation and enforcement of IT security policies, supporting guidelines, and processes to assure the security of information and information system resources. The Agency implemented contracts that provide penetration testing as well as incident handling/ response services on a 24/7/365 basis. During FY 2002, the Agency developed performance measures for Agency goals, including target performance levels, which are reviewed and approved quarterly by the Administrator. Security reviews were conducted on all five Agency components.

Security Awareness Training is required training and must be taken by all Agency associates and contractors. However, the Agency reported that of the 17,196 employees and contractors, 87% received security training. As of the date of the report, none of the 188 employees considered to have significant security responsibilities had received specialized security training. The training of these employees was scheduled to be completed by the end of the calendar year. Total costs expended for the IT security training of Agency employees and contractors exceeded $750K, nearly a 300% increase over FY 2001 security training expenditures.

2. CIO methods to ensure contractor services are secure.

The IG evaluated security for the Agency's Nationwide Information Infrastructure (NII) and determined that background investigations had not been conducted for contractors supporting the NII. Pursuant to this investigation, the IG reported that the Agency was developing an action plan to include background investigation requirements for contractors providing NII services.

The nationwide Blanket Purchase Agreement for IT services contains strict contract language in the Statement of Work documents that outlines explicit contractor and third-party security requirements. The CIO performs network logging and auditing including the use of Intrusion Detection Systems, contractor authorizations with minimum background investigations, and auditing of contractor activities to assure that services provided by contractors and consultants are secure.

3. Agency integration of security and capital planning.

During FY 2001 and FY 2002, the IG reviewed 12 systems of which eight had completed security plans and five had completed risk assessments. For the 12 systems reviewed, the

Control phase indicated that ten were within project cost, on schedule, and had no performance problems. The other two systems reviewed indicated that there were significant variances from planned performance measures. The IG noted that these reports are not intended to monitor security activities for Agency systems. The IG expressed concern that the newly implemented capital planning and investment control policy did not include a description of the working relationship between the project manager role that has been identified and other security positions already established for the Agency. The IG stated that "clarification of agency-wide IT security roles and responsibilities within GSA's IT Security Program Plan is needed to ensure that security is fully integrated into GSA's capital planning process."

The Agency developed the CPIC process that specifically includes IT Security and IT enterprise architecture. The CPIC process ensures that all Agency IT acquisitions are tightly coupled with their required security controls to effectively manage risk. The process outlines three main CPIC phases: Select, Control, and Evaluate.

The Agency reported that 41 capital asset plans and justifications were submitted to OMB in the FY 2003 Budget Materials. As of the date of the report, the Agency's FY 2004 Budget Materials had not been submitted to OMB. However, the IG indicated that the Security Division had reviewed 22 FY 2004 budget submissions for security and privacy content.

National Aeronautics and Space Administration (NASA)

A. General Overview

1. Security funding.
The National Aeronautics and Space Administration reports planned FY 2003 funding for IT security and critical infrastructure protection of $88M. This funding level comprises 4% of their total planned IT portfolio of $2.02B.

2. Number of programs reviewed.
The IG reviewed 77 out of 1,666 systems. Many of their reviews did not relate to specific systems but covered groups of systems or capabilities that involved the agency-wide network. In FY 2002, NASA reported a total of 1,641 systems, of which a total of 1,494 were "checked".

OMB requires that agencies use the National Institute of Standards and Technology (NIST) publication guidance to review their systems, unless the agency-developed methodology contains all elements of the NIST guide. NASA used its NASA Procedures and Guidelines (NPG) 2810.1 document to cover the Agency's information technology security requirements. The IG reported that it contains about 85% of the NIST guidance. It does not address the detailed level for system reviews as discussed in NIST, nor does it contain the NIST requirement to test and evaluate security controls. NASA reports that while it did not use the NIST self-assessment guide in its program reviews, it was used as the basis for the

items on the NASA standard IT security weakness list in the Agency's Plan of Action and Milestones (POA&M) report.

3. Material weaknesses.
The IG reported that NASA had not successfully implemented, monitored, or enforced its program because until very recently, the Agency lacked centralized IT leadership. The IG continued to find weaknesses similar to those found in the FY 2001 report including, inadequate security training for systems administrators, and an inconsistently applied program for ensuring security of sensitive systems, an inadequate enforcement mechanism to ensure that host and network security policies and procedures are appropriately implemented, and outdated security plans for NASA's IT-related systems, as well as an inadequate incident response capability. Additional FY 2002 weaknesses included the Agency's procedures for the removal of sensitive information from electronic devices and for the use of authentication tokens. In addition, FY 2001 and FY 2002 financial audits found similar weaknesses including inadequate disaster recovery testing and inadequate logical access controls. The IG, therefore, again finds NASA's IT security program to be a material weakness.

NASA reported that the Administrator continues to review weaknesses that have been identified through various audits, inspections, and reviews of the Information Technology Security (ITS) program and has determined that while IT security remains an area of significant management concern, none of the weaknesses are classified as being material.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG reported that although the policies and procedures provide direction to ensure that safeguards for the protection of the integrity, confidentiality, and availability of IT resources are integrated into and support the missions of NASA, weaknesses they discovered problems with implementation of those policies and procedures.

The Administrator created the Office of Security Management & Safeguards, which is responsible for establishing the certification and accreditation policies, procedures, and guidance for all classified IT systems operations. Since the Centers have the responsibility to meet the needs of their users within a unique, program-specific environment, IT investment decisions are made at the Center level. Each Center has a Program Management Council (PMC), in which the Center CIO is a key member. These decisions are made strictly within the context of the approved budget and IT security plans.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
In FY 2001, the IG recommended that the Agency establish a performance measure to determine if IT security is planned throughout system life cycles and maintained in FY 2002 that the Agency still needs to establish such a performance measure. In its third quarter FY 2002 POA&M, NASA reported that it had completed actions pertaining to the establishment of a performance measure in this area. The IG disagreed.

As of June 17, 2002, NASA had identified 1,666 operational systems, significantly reducing the number of operational systems without security plans from 546 (35 percent of the 1,550 operational systems in FY 2001) to 195 (12 percent of the 1,666 operational systems in FY 2002). The IG raised concerns over the performance of the Centers in maintaining their system inventories to help track progress made in life-cycle requirements and additionally found that some Center system inventories omitted non-operational systems or may not have included all systems.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG reported that NASA integrated its IT security program with its critical infrastructure protection responsibilities and other security programs by establishing distinct roles for the CIO and the Critical Infrastructure Assurance Officer (CIAO). The IG found good coordination between the two.

4. Critical asset prioritization and protection methodologies.
As of August 2002, the IG found that NASA had not taken sufficient actions to accurately identify all mission essential infrastructure (MEI) assets. In the POA&M for the FY 2002 third quarter, NASA stated, "Guidance has been issued and requests for changes to the MEI list using new update procedures are coming in from the Centers" and that the Agency considers the matter closed. The IG disagreed because the Agency had not yet updated the MEI list. The IG stated that without an accurate identification of MEI assets, NASA may not be adequately protecting its entire critical infrastructure.

5. Department documented procedures for reporting and sharing vulnerabilities.
The Administrator through the Agency CIO assigned to the Principal Center for IT security (PCITS) responsibility for agency-wide reporting, tracking and responding to incidents. NASA created a centralized reporting structure across its eleven Centers for measuring performance and evaluating efforts undertaken to protect against cyber attacks. Each NASA field Center and HQ has responsibility for reporting computer crimes to the Office of the Inspector General Computer Crimes Division, which reports the incidents to law enforcement authorities or conducts its own criminal investigations.

The IG recommended that NASA improve its incident response capability to ensure accurate reporting of unclassified IT incidents. NASA's Incident Response Center (NASIRC) records for many types of IT security incidents did not identify when the incident occurred or when the incident was reported to Center officials, law enforcement, or FedCIRC. For 136 incident records that the IG traced from NASIRC to Center records, 74, or 54% of the records, contained errors. The errors included incorrect incident categories and duplicate entries. The structure and content of the IT incident database limited NASIRC's ability to compile meaningful analyses and reports on potential threats and incident trends. Because of inaccuracies and difficulties with the database, the IG maintained that NASA underreported the number of security incidents to FedCIRC, and provided incomplete and unreliable incident information to the FedCIRC. The IG also continued to be concerned about the timeliness of NASA's response to IT security incidents.

NASA was in the process of improving its reporting mechanisms by implementing a Web-based incident reporting system that will be able to provide information on each of its systems in near real time. In addition, to track and manage incidents more effectively, NASA is developing an innovative centralized system known as the NASA Cyber Attack Response System (NCARS). It is designed to identify, correct and report incidents of all attacks on NASA systems, showing on a continuous basis the status and type of all reported incidents throughout the Agency.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.

The IG reported that the Agency initiated a phased approach for developing IT security plans for six types of systems. During FY 2002, the IG reviewed 27 systems to determine whether program officials performed risk assessments, determined level of security, maintained current security plans, and tested and evaluated security controls.

In FY 2001, the IG reviewed security plans for 49 systems and in FY 2002, plans for 27 systems were reviewed. Of these 27 systems, 26 were assessed for risk, with 21 of them having been assigned a level of risk after a risk assessment had been conducted. Twenty-five of the 27 systems had an up-to-date security plan and 25 systems had been authorized for processing following certification and accreditation. Two were operating without written authorization. None of the 27 systems had the costs of their security controls integrated into the life cycle of the system. Fifteen of the 27 systems had security controls that had been tested and evaluated in the last year. Twenty-five systems had a contingency plan but only 18 of those 25 contingency plans had been tested in the past year.

2. Department methods to ensure contractor services are secure.

In FY 2002, NASA reported reviewing all 251 of its contractor operations or facilities. The IG noted that NASA made considerable progress in incorporating an IT security clause into applicable unclassified contracts and purchase orders. In addition, NASA modified its Grant and Cooperative Agreement Handbook to require the IT security clause in cooperative agreements and was revising the Handbook to include the clause in grants. In its FY 2002 third quarter POA&M, NASA reported that the IT clause had been implemented in about 96 percent of its contracts.

The IG reported that issues remain concerning the submission of contractor IT security plans as required under the NASA Federal Acquisition Regulation (FAR) Supplement clause. The supplement states that the contractor shall be responsible for IT security for all systems connected to a NASA network or operated by the contractor for NASA regardless of location. It also requires the contractor to provide, implement, and maintain a NASA-approved IT security plan; screen personnel requiring privileged access to systems operated by the contractor for NASA or interconnected to a NASA network; ensure its employees receive annual IT security training in NASA's IT policies and procedures; and incorporate the IT security clause in all applicable subcontracts. The IG stated that required plans were

not submitted for all applicable contracts and inconsistencies exist agency-wide regarding the due date to submit the plans and the identification of NASA officials who must review and approve the plans.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
In FY 2001, the IG reported that the performance measures for IT security awareness and training, vulnerability reduction, incident response, and policies and procedures were inadequate. In its third quarter FY 2002 POA&M report to OMB, NASA reported that the related weaknesses had been corrected. The IG's review of these areas in FY 2002 identified continuing weaknesses.

NASA's IT security program requires civil service and contractor users to complete IT training before they can be authorized access to any NASA IT system. The IG found only 5 of 13 awareness and training-related metrics for FY 2002 required all users to complete the required training. In FY 2001, the IG noted a particular concern that the performance measure for system administrator training excluded contractor personnel, who composed about 79 percent of NASA's system administrators.

2. CIO methods to ensure contractor services are secure.
The majority of NASA's IT operations and assets are under the control of program officials, not the NASA CIO. The IG did not review contractor operations and assets under the control of the Agency CIO.

NASA reported that for those operations and assets under the CIO's control, the CIO established specific actions to ensure that services provided by contractors or another Agency are appropriately secure. In so doing, the CIO ensures that they meet the requirements of GISRA, OMB Policy, NIST guidelines as embodied in Agency guidance, thereby meeting Agency policy.

Of it 251 FY 2002 contracts, NASA reported that all had been reviewed by the Center CIO to determine the appropriateness for inclusion of the Agency prescribed security clause. This clause has been added as a non-negotiable clause in all new contracts. Of the 251 existing contracts, 240 of them have had the security clause added. IT security training was mandated for all contractor staff to ensure that both overall awareness and specialized training are applied equally to contractor and Agency staff.

3. Agency integration of security and capital planning.
The IG reported that generally, NASA integrated security into the Agency's capital planning and investment control process. NASA reported that every capital asset plan and their Exhibit 53 submitted to OMB included security requirements and costs and that the CIO and other appropriate officials independently check all capital asset plans.

National Science Foundation (NSF)

A. General Overview

1. Security funding.
The National Science Foundation reports planned FY 2003 funding for IT security of $3.96M. This funding level comprises 10% of their total planned IT portfolio of $40M.

2. Number of programs reviewed.
In the FY 2002 report, the Agency reviewed only their major systems. GISRA requires agencies to review all systems each year and does not draw a distinction between major and non-major systems. The IG reviewed seven systems and, although all elements of the NIST self-assessment guide were generally addressed, recommended that the Agency strengthen its process for tracking and addressing weaknesses identified by the self-assessments. The Agency used the NIST Self-Assessment Guide (SP 800-26) for consistency and effective assessment of the overall security program.

3. Material weaknesses.
The Agency reported no weaknesses in policies, procedures, or practices that materially impact the effectiveness of the entity-wide security program. However, the IG identified ten findings of which three were classified as "significant deficiencies" and seven were noted as "other matters" that, although not classified as significant deficiencies, may have a detrimental effect on the Agency's security program. Agency management generally agreed with the IG's findings and recommendations; it disagreed with the assessment of the significant weaknesses and contends the deficiencies do not represent a weakness in a policy, procedure, or practice that materially impact the security program's effectiveness. As such, the Agency did not include these in a classification of "material weakness."

The three weaknesses the IG identified include: critical internal applications are vulnerable to unauthorized modification, viewing and deletion of data; weaknesses in the Agency's security management structure and the lack of system certifications and accreditations.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG recommended that the Director "formally establish a security management structure to ensure that responsibilities and related authorities required by GISRA are assigned and delegated." The Agency concurred with this finding and separated the Director of OIRM and CIO positions and appointed the Director of the Division of Information Systems as the Deputy CIO. Additionally, the Director created and filled an agency Security Officer (SO) position, appointed a new CIO, and provided for the establishment of an agency-wide security working group to support the CIO in implementing the Agency's security program.

During FY 2002, the Director issued a memorandum to the Director's Policy Group that the CIO would be working with each organization to review security needs of all systems and that the CIO would work with programs to ensure that all aspects of GISRA were being implemented throughout the Agency. The CIO ensures that the security plans for each agency system are consistent with the Agency's agency-wide security policy and guidelines. Although the Agency has a cadre of staff performing a variety of security duties, their responsibilities and requisite levels of authority were not formally recognized and communicated in the Agency's policies and procedures, organization charts, delegations of authority, and individual position descriptions.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.

The IG's concern, as previously mentioned, was that they consider the Agency's security management structure to be significantly deficient. They report that the lack of a comprehensive security management structure poses significant risks to the Agency's ability to implement, monitor, and review its entity-wide security program and to maintain an effective control environment. The IG was concerned that, until the security management structure is strengthened, the Director's ability to ensure that the security plan is practiced throughout the life cycle of each system could be hindered. The IG acknowledged that the Director issued memoranda emphasizing the CIO and SO roles and responsibilities and made several significant security related organizational changes that should enhance the Agency's security program.

The CIO was delegated the primary responsibility for development and maintenance of the Agency's Information Security Program, which includes oversight and review of the implementation of the GISRA requirements throughout the life cycle of the corporate systems maintained and operated by the directorates and offices. The CIO ensures that the security plans for each agency system are consistent with the Agency agency-wide security policy and guidelines. The Director, through periodic management reviews with the CIO and the Director's Policy Group, oversees the progress of the CIO in reference to the delegated duties relating to the implementation of the GISRA requirements. Through this oversight, the Director is able to reinforce the requirements of the Agency's security program and provide formal memoranda pertaining to such, if the need arises.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The Agency has a single integrated information and IT security program and has very limited critical infrastructure protection (CIP) reporting requirements and responsibilities. Although this was the original understanding of the IG, a GAO issued report in FY 2002 described the Agency's CIP responsibilities relating to computer security education and research. The IG indicated that the Agency had not integrated its CIP responsibilities with its entity-wide security program; however, the new agency-wide security working group will provide a forum to communicate security-related initiatives, which includes CIP research initiatives that may have potential impact on the Agency's operational security program.

Corporate application systems, corporate infrastructure, and network operations are centrally managed. For those few systems not centrally managed, the program offices assign system administrators and database administrators to maintain administrative security over the individual systems. The Agency maintained that there is no unnecessary duplication of overhead costs, and the policy and procedures are consistent and complementary across the various programs and disciplines. This is confirmed by the IG's observation that the cooperation between the Agency's Administrative Services and Information Systems Divisions reduces the overhead costs of two distinct checkout procedures and provides improved security.

4. Critical asset prioritization and protection methodologies.
Critical infrastructure responsibilities of the Agency are focused on research and development rather than the protection of national critical infrastructure. Under these circumstances, a Project Matrix review is not required. However, the Agency developed a process for identifying critical information technology operations and assets that requires system owners to conduct risk assessments. Using these criteria, major and non-major systems were identified, classified, and documented. The Agency required major system owners to complete the NIST Self-Assessment and to have an updated security and contingency plan. The IG advised that these security plans were developed for all major applications and general support systems and that "these plans help identify interdependencies and interrelationships and describe, at a high level, how the systems are secure."

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG reported that the Agency needs to fully implement a software patch management process whereby vulnerabilities are identified and related patches are tested and applied in a timely manner.

Incident reporting procedures were fully documented and a process was established with the IG to investigate security incidents, communicate with law enforcement and FedCIRC, and notify system owners. The Agency established a Computer Incident Response Team (CIRT) to implement this process. An incident report must be completed for all security incidents that are communicated to FedCIRC. The Agency indicated that incident information is shared with FedCIRC and that an average of six hours is required to report such incidents. For FY 2002, 12 incidents were reported at the agency level with one incident being reported externally to FedCIRC or law enforcement. Weekly meetings of IT staff aids in sharing information on security alerts and the Agency has contracted with an independent vendor to provide 24/7 managed-intrusion detection services.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
As reported, many of the agency's major systems had not been certified and accredited. The IG identified this as a major deficiency and included other areas such as, security plans that did not identify application controls and fully describe the operating environment, and risk

assessments that did not identify application specific vulnerabilities and associated risks. The IG also noted that, during their review of FY 2002 self-assessments for seven major systems (one general support system and six major applications), the NIST self-assessment templates were completed, but analyses of the results, areas for improvement, and the overall risk level for each major system were not identified and defined.

The Agency reported that 55% of the major systems had a contingency plan in effect, but only 45% of the major systems had the contingency plan tested in the past year. The Agency advised that, with a new Agency-wide information security policy and a companion information security handbook, the Agency plans to certify and accredit all major systems, including those that have been previously certified and accredited. The Agency plans 100% completion of this goal in FY 2003.

2. Department methods to ensure contractor services are secure.
To better ensure the Agency's critical assets and networks are protected, a 24/7 managed intrusion detection service was procured and implemented. Immediate alerts are provided to the Computer Incident Response Team (CIRT) when potential or actual external intrusions or attacks may occur. All Agency contracts include clauses that stipulate that contractor-developed or contractor-provided services must conform to Federal security guidelines and mandates. Program officials of the Office of Polar Programs (OPP) worked collaboratively with the U.S. Antarctic Program (USAP) contractor in performing security reviews of contractor operated sites and systems and have completed three of nine planned site assessments and the corresponding NIST self-assessments.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG advised that the Agency CIO made progress in information security areas; however, the IG also pointed out that additional actions are necessary to further strengthen this program. The IG further stated that "the basis for any security program is a well-defined and promulgated entity-wide security policy combined with senior management sponsorship." Although the Agency documented security procedures in its Security Handbook, and promulgated policies on virus protection and GISRA program reviews, it had not established and promulgated an entity-wide security policy by which program officials are held accountable for security performance.

During FY 2002, the CIO made progress in developing and implementing an entity-wide information security program. Among these accomplishments were: an extensive review of all system resources to assure compliance with GISRA; review of risk assessments and plans; issuance of Agency-wide security policy and procedures; creation and successful recruitment of an entity-wide Security Officer; and implementation of additional management, technical, and operational controls. The CIO established required Agency-wide security awareness training to assure that all employees and on-site contractors were aware of their responsibilities for security. Ninety-one percent of the employees and contractors received this training during FY 2002. The CIO provided additional security seminars and training for

those staff members and contractors (20 out of a total of 22) that have specialized IT and significant security responsibilities.

2. CIO methods to ensure contractor services are secure.
The CIO did not have any contractor-managed services or services provided by other agencies under their control. As the CIO is responsible for ensuring that program officials implement the requirements of GISRA in contractor-operated facilities, several initiatives to assure these contractor-managed services are adequately secure have been implemented. Full-time permanent contractors working on-site or on critical systems undergo background checks as a normal part of the contracting process in addition to taking the required security awareness training.

3. Agency integration of security and capital planning.
The IG revealed that, although security controls and related costs over the life cycle of each system had not been explicitly laid out, the CIO had reported the necessary information relating to security controls and costs for submitted budget materials. The CIO reported that the Agency's capital planning document stipulates that information security policies, procedures, and practices must be addressed as part of overall capital planning and investment control. Security costs, as a percentage of the total costs for IT capital projects, were reported by the Agency.

Nuclear Regulatory Commission (NRC)

A. General Overview

1. Security funding.
The Agency reports planned FY 2003 funding for IT security of $2.1M. This funding level comprises 3.1% of their total planned IT portfolio of $66M.

2. Number of programs reviewed.
The IG's report indicated that self-assessments were provided on 15 systems. The Agency has only one integrated automated information system security program that has responsibility for the entire organization. The Agency identified and reviewed18 systems in FY 2002. The Agency used the NIST self-assessment guide for the FY 2002 security program evaluation.

The IG reported that the Agency began conducting self-assessments on additional systems owned by the Office of Nuclear Security and Incident Response (NSIR) in FY 2002. NSIR system owners did not report in the FY 2002 GISRA evaluation because they believed their systems did not meet the criteria for the Agency systems that required protection. The Agency has now required the NSIR be included in the GISRA self-assessment process.

3. Material weaknesses.

The IG's independent evaluation indicated that "while the NRC had made substantial progress in remediating several fundamental weaknesses identified in the 2001 GISRA evaluation, the evaluation found that the NRC security program is not well integrated and not consistently implemented across the enterprise." The IG maintained that due to the lack of integration and inconsistent implementation of security programs, the Agency may not be able to determine the level of risk at the enterprise level. The IG recommended that enhancements and consistent implementation of security elements receive high priority to increase the Agency security posture across the enterprise. The Agency reported that they have no conditions that meet the criterion of a material weakness for FY 2002.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The IG reported that the IT security program is not being implemented on a consistent basis across the Agency. The Agency requires project managers to account for security related activities in their respective projects. During the FY 2002 IG independent evaluation, the IG found that IT investments in excess of $500K were approved without having a business case or having going through the proper capital planning and investment control process. The IG recommended that the Agency conduct an agency-wide evaluation to determine the consistency of IT investment policy implementation.

The Agency approved and established a Senior Information Technology Security Officer (SITSO) position in FY 2002. The SITSO reports directly to the CIO and is responsible for oversight of the agency-wide IT security program. The SITSO is responsible for assuring that the Agency's IT Security Program meets and complies with the requirements set forth in the GISRA.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG report indicated that the Agency lacks current information on all Agency systems and may not be aware of systems that have special security requirements or be aware of systems whose documents are not up-to-date or are incomplete. The IG's review found that the System Development and Life-Cycle Management (SDLCM) methodology does not address security in the design phase, testing phase and ongoing maintenance phase, nor does it address the certification and accreditation required for new systems or major system upgrades. The methodology did not integrate the security life-cycle with all phases of the system life cycle. Recent policy and procedure changes may not be included in the management directives and, thus, system owners may not be aware of changes to IT security policy and procedures

The CIO and agency program officials were tasked by the agency head to complete all steps necessary to bring their major application and general support systems into compliance with policy and guidance. Updated security plans were also to be in place by July 2002. The Office of the CIO reviewed the security status of all Agency applications and systems, of which status information is now included in an Information Technology Security Tracking

System (ITSTS). The ITSTS will monitor review schedules and help ensure that the status of outstanding security actions are known and monitored.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG indicated that there is no clear definition of roles, responsibilities, and authorities of different Agency security program officials. The lack of clear definitions could result in increased security costs and possible duplication of, or limitations to, security controls.

The Agency has one, comprehensive and integrated security program, which includes integration of the critical infrastructure protection responsibilities. The Agency reported that this prevents unnecessary duplication of security staffs and overhead costs. A Personnel Security Program provides for background screening for all Agency personnel and contractors commensurate with their level of access to sensitive IT systems and data. The Agency and IG both contend that the Agency does not have a national role relating to critical infrastructure protection. PDD 67, "Ensuring Constitutional Government and Continuity of Government Operations," does require the Agency to respond on two minimum essential functions, i.e., nuclear incidents and emergency decision-making. Periodic reviews of functions and systems in conjunction with the Continuity of Operations Plan (COOP) are being conducted by the Agency which enables the Agency to fulfill the most important functions in the event of any major disruption of service.

4. Critical asset prioritization and protection methodologies.
The Agency initiated a review to provide additional insight into its critical assets and systems to determine if there is a need for additional protection. Contingency planning is performed from two perspectives: continuity of operation and backup and recovery. Both the Agency and IG agree that the Agency planning mechanisms ensure the restoration of normal operations as soon as economically feasible in the event of a system failure and that the Agency management is kept aware of critical resources, functions, and continued operations should such event occur.

5. Department documented procedures for reporting and sharing vulnerabilities.
The NRC developed and implemented information systems security incident response procedures during FY 2002. A Computer Security Incident Response Capability (CSIRC) team was established by the Agency and prepares periodic reports that are submitted to the Agency and FedCIRC, if necessary. Incidents are evaluated on a 5 tier system with level 4 (Damage) and 5 (Exploit) incidents being immediately forwarded to FedCIRC. The Agency, in cooperation with the IG, coordinates any incidents that may require the assistance of or involvement with appropriate law enforcement authorities. Based on the implementation of this new process, the Agency had not yet had to provide a report to FedCIRC. There had been a significant increase in the number of incidents reported in FY 2002 (7,508) as compared to FY 2001 (198). The IG indicated that this is a direct result of additional automated intrusion detection systems that were brought on-line during FY 2002 and include routine probes and scans that are constantly being conducted on organization networks and systems that have Internet connectivity.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.

The IG expressed concern that only six systems had a current security plan. Three systems had draft security plans, four had three-page security plans that do not adequately address the requirements of a security plan, and three plans were out-of-date. The Agency program officials, according to the Agency, had taken appropriate steps to assure that all systems will be in full compliance with GISRA, OMB, and NIST security requirements. The Agency reported that 100% of the Agency's systems had been assessed for risk, had been assigned a level of risk, and had an up-to-date security plan. However, only 50% of the systems had been certified and accredited. The IG reported that seven of the 15 systems are operating without a contingency plan, and certification and accreditation. According to the Agency, formal approval to operate was on track for completion by the end of FY 2002 for the remaining systems. The Agency's report indicated that 13 of the 18 systems had a contingency plan in effect but that only seven of these had been tested in the past year. The IG's report indicated that 13 of 15 systems had a contingency plan but that only one had been tested in FY 2002. The IG recommended that NRC test contingency plans at least annually and that they complete contingency plan testing on all major applications and general support systems.

2. Department methods to ensure contractor services are secure.

The IG was unable to obtain a copy of a Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), or other agreement that assures adequate security of the external entities. In addition, there was no Agency policy for performing periodic vulnerability assessments of their respective systems. The IG expressed concern that this inadequacy may result in increased vulnerabilities to the NRC systems.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.

The IG found a lack of effective communication between the regional offices, the Technical Training Center, and Agency headquarters regarding the implementation of Agency information security programs. No reviews or audits had been conducted on the regional offices or TTC to assess their compliance with the agency-wide IT security program. The Senior Information Technology Security Officer (SITSO) had begun adopting a more proactive oversight program to assure compliance with the agency-wide security program. The IG reported on numerous deficiencies on security control testing including: password management, login management, system auditing, remote access service procedures, software maintenance, data communication network safeguards, and hardware and software inventory.

The Agency reported that with the recent appointment of the SITSO, the CIO is now capable of performing the oversight tasks required to adequately maintain an agency-wide security program. The IG concurred that the Agency had made improvements in their security

posture, and had taken additional steps to ensure the effective implementation and evaluation of their security program.

The percentage of employees and contractors receiving security training during FY 2002 decreased from that reported in FY 2001. Twenty-two percent of the 4,769 employees received the training in FY 2002 at a cost of $68.7K. Of the 4,826 employees reported in FY 2001, 24% received training at an estimated expense of $30K. The IG recommended a more stringent training program for system security officers (SSO) and points out that the lack of adequate training reduces the efficiency of the SSO's performance.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
The Agency reported that security had been fully integrated into the Agency's capital planning and investment control process. For all business cases submitted for IT investments, security is a major consideration that is specifically reviewed during the screening process. Both the IG and Agency reported that the NRC reported its security requirements and costs on every FY 2003 capital asset plan. The Agency is following and adhering to the guidance in the preparation of OMB Exhibit 300 and Exhibit 53s as defined in OMB Circular A-11, "Guidance on Preparing, Submitting, & Executing the Budget."

Office of Personnel Management (OPM)

A. General Overview

1. Security funding.
The Office of Personnel Management reports planned FY 2003 funding for IT security and critical infrastructure protection of $6M. This funding level comprises 4.4% of their total planned IT portfolio of $135M.

2. Number of programs reviewed.
Information provided to the IG from the Agency, at the time of the IG's review, indicated that the Agency did not provide a systems inventory for FY 2001 or FY2002. The IG performed independent evaluations on five major application reviews and two general support system.

OPM reported that they identified all systems and reviewed all programs in F 20Y02. They reported 14 agency programs with 42 agency systems. OPM's report indicated that all 14 agency programs and 24 of the 42 systems were reviewed in FY 2002.

OPM used the criteria established in OMB Circular A-130, Appendix III in the evaluation of the various systems. In addition, the NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," and NIST Special

Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," were used in the review.

3. Material weaknesses.
As in the FY 2001 report, the Agency and IG reported no weaknesses as a material weakness. However, the IG did note several areas that they would consider as "reportable conditions."

B. Responsibilities of the Agency Head

1. Measures of performance used by the Agency to clearly set forth the Security Act's responsibilities and authorities for the Agency CIO and program officials.
The IG's report indicated that the Agency CIO needs to take a more proactive leadership role in working with program office heads and their staff to understand their system security responsibilities and implement effective information security programs as set forth in GISRA. The IG also indicated that while there is no formal process in place by which the CIO reviews and approves all IT expenditures, there is informal coordination between the agency program offices and the CIO on IT procurement.

According to OPM, their IT Security Policy clearly and unambiguously defines the IT security roles, responsibilities and authorities for OPM's managers, program officials and staff. The Director charged the CIO, as reflected in the IT Security Policy, with agency-wide IT Security Program oversight and leadership responsibilities. The Agency reported that all IT investment decisions are reviewed by the CIO or senior advisers who provide the CIO advice and guidance on investment decisions. No major IT investment proceeds without the concurrence of the CIO.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Agency developed a standard system development life cycle (SDLC) methodology. However, at the time of the FY 2002 report, the system had not yet been considered as "fully functional." An Information Technology Systems Manager (ITSM) had been implemented by the Agency and all IT system developers will be required to utilize this system throughout the life cycle of each system. The IG was unable to verify that all appropriate program offices employed the use of ITSM, due to the on-going implementation of the program. However, the IG did recommend that the CIO finalize the development and implementation of the ITSM methodology, develop and implement management controls to ensure that all new system development and significant system maintenance within the Agency use the ITSM methodology and, develop a process by which ITSM users can request enhancements to the tool's functionality.

The Director delegated oversight of the program official's IT security responsibilities to the CIO. As part of the annual GISRA review process, the CIO provided a comprehensive IT Security Guide to all program office heads. Based on the responses from the program offices, the CIO now has a baseline for monitoring progress toward meeting the goal of having all systems certified and accredited with up-to-date security plans and having security integrated throughout the system life cycle.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.

The FY 2002 report from both OPM and the IG indicated that there has been no integration of IT security programs with critical infrastructure responsibilities. The Agency does report, however, that many of the critical infrastructure protection plan elements have been incorporated into the Security Program. The OCIO is working in conjunction with the Office of Contracting and Administrative Services, which oversees non-IT security, to provide for a fully synchronized disaster recovery plan. The IG advised that while this program appears to be consistent with the requirements of a critical infrastructure plan, the Agency is only in the initial stages of implementing the IT security program.

4. Critical asset prioritization and protection methodologies.

The Agency reported that they have not undergone a Project Matrix review and do not have plans to do so as a Project Matrix review would be inappropriate for the Agency's environment. They do contend that they have controls in place to identify, prioritize, and protect critical operations and assets within their enterprise architecture. The IG indicated that the agency lacks a disaster recovery plan for the Network Management Center's network operations. The IG concurred with the report of the Agency and identified several additional areas of lax security requirements in addition to strongly encouraging the Agency to implement recommendations and correct noted deficiencies. The IG recommended the completion of security plans for the two general support systems and all major application systems. The Agency reported that by accomplishing the development of information system security plans for their two major infrastructure components, they will fulfill the requirements to identify the critical operations and assets, their interdependencies and interrelationships, and how they intend to secure the agency operations and assets.

5. Department documented procedures for reporting and sharing vulnerabilities.

The FY 2001 review indicated the Agency had not yet identified the Computer Incident Response Team (CIRT) members. The same holds true for FY 2002 and is confirmed by the IG. The Agency reports a total of 14 agency components with one having incident handling and response capability. The IG reported that the Agency's Helpdesk is unaware of formal procedures for handling security incidents and that agency employees have not been effectively informed of IT security procedures. According to the IG, the Agency's security procedures do not require notification of the Agency's IG concerning security incidents as required by OMB Security Act implementing guidance. The IG is concerned that with the Agency's lack of full implementation of security incident handling procedures, there is a higher risk that such incidents may not be properly handled and reported.

One security incident was reported by the Agency and the incident was not reported to FedCIRC. The Agency advised that they will subscribe to the FedCIRC sponsored Patch Authentication and Dissemination Capability when it becomes available and that it should improve the agency's ability to track and ensure that patches are installed and tested in a timely manner. The current primary method of confirmation is through the periodic running of vulnerability scans to determine where there are missing up-to-date patches.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reported that, while the Agency had clearly made progress in implementing its IT security policy, much work remains to be done, i.e. no program offices had assessed the risk to operation and assets under their control. Further, none of the program offices had security plans for the systems under their control and none of the systems had been certified and accredited to operate.

While the Agency reported that it has made progress in implementation of its IT security policy, they also report that none of the program officials have assessed the risk to operations and assets under their control. All 42 systems were operating without written authorization and only five have been assessed for risk. Six systems were reported to have a contingency plan in effect and all had the contingency plan tested in the past year.

2. Methods to ensure contractor services are secure.
The Agency had imparted measures and adequate controls to help ensure that contractor services are performed in accordance with the requirements of GISRA. One area of concern was expressed by both the IG and OPM that referenced a lack of adequate controls for deleting system access for contractors when they leave the agency. Areas where the Agency reported that they are performing adequately include contractor supervision in accordance with Agency regulations, unique user IDs for accountability, completion of an access request form before data is transferred, and all data transferred to and from the Agency must be encrypted.

D. Responsibilities of Agency Chief Information Officer

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG reported that the Agency had not fully implemented an agency-wide IT security program and while staff members with significant security responsibilities receive IT security training, there is no formal training plan for all employees. The Agency developed several security plans which address existing IT security requirements such as risk management, information system security plans and certification and accreditation. Although the Agency developed these plans, no systems have been certified and accredited. Although the Agency provided information pertaining to the total number of employees and contractors in the agency, they did not provide the total number and percentage of employees and contractors receiving training, total number of employees with significant security responsibilities or, type of IT security training available. The Agency reported security training costs for FY 2002 totaled $59K.

2. Methods to ensure contractor services are secure.
The IG reported that the Agency did not provide the IG with specific performance measures required by GISRA. According to the IG, "weak controls related to contractor identification increase the risk of unauthorized access to sensitive systems and data." OPM reported that

their security controls for contractors are the same as that for Agency employees. The Agency's IT security policy requires that all contractors undergo background security clearances.

3. Agency integration of security and capital planning.
The IG reported that the integration of the security requirements into the capital planning process cannot be substantiated by documentation submitted to them by the Agency. The Agency submitted two capital asset plans to OMB for the FY 2003 budget and six for FY 2004. The Agency reported that they have integrated security requirements and cost estimates into the capital planning and investment control process and these costs were reported in the agency's Exhibit 300 and Exhibit 53.

Small Business Administration (SBA)

A. General Overview

1. Security funding.
The Small Business Administration reports planned FY 2003 funding for IT security and critical infrastructure protection of $4.45M. This funding level comprises 7.3% of their total planned IT portfolio of $61M.

2. Number of programs reviewed.
Using the process and checklist found in NIST SP 800-26, SBA conducted self-assessments on seven agency programs and reviewed all 37 of its systems.

3. Material weaknesses.
In FY 2002, SBA was considering any significant vulnerability highlighted in its May 2002 IG report. SBA, therefore, reported six material weaknesses in FY 2002. These include inadequate intrusion detection systems and failure to consistently report security incidents, weak security controls including identification and authentication and separation of duties on individual systems, inadequate system testing and evaluation, inadequate disaster recovery and contingency planning and testing, inadequate certification and accreditation, and limited supervision of contractor provided services.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The Administrator drafted a memorandum that sets forth duties and responsibilities for SBA program officials. The draft that was in the process of being finalized at the time of the IG evaluation stated that the Office of the CIO will continue to lead SBA's initiative to enhance the Agency's computer security program and its responsibilities under GISRA. In the mean time, SBA Standard Operating Procedure 90 47, *Information System Security Program*, stated that the Administrator delegated to the CIO responsibility for establishing a

management control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications. The CIO ensures compliance with SBA infrastructure and architecture standards and advises the SBA Business Technology Investment Council (BTIC) on technical matters. The BTIC, chaired by the CIO, is responsible for reviewing and making decisions on all major IT investments, including screening; scoring, and prioritizing new initiatives, monitoring ongoing investments, and evaluating implemented investments. A major operating component of the Agency cannot make a significant IT investment decision without review by and concurrence of the BTIC.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported that SBA had not established through a Standard Operating Procedure (SOP) how security will be enforced for SBA systems throughout a system's life cycle. An information notice was issued in November 2001 that requires all internally developed systems to follow the Agency's Systems Development Methodology (SDM); however, no SOP covers the broad areas of systems development or acquisition. As part of SBA's "Ten Management Challenges," the IG recommended that such an SOP be developed.

During the FY 2002 reporting period, the CIO, in concert with SBA program officials, prepared system security plans for seven additional SBA systems as compared to the FY 2001 totals. After the initial three-year certification, accreditation, risk assessment, and system security plan creation for all SBA systems, the CIO stated that it will be the responsibility of the SBA system owners to schedule, fund and create or update their own system security plans. This initial accreditation procedure was funded through the Office of the CIO so that a formalized approval process could be created with baseline security documentation created.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG stated that prior to March 2001, SBA did not include protection of physical assets in its Critical Infrastructure Protection Plan (CIPP). In response to the IG findings in this area, SBA named a Deputy Chief Infrastructure Assurance Officer (CIAO) for Physical Infrastructure. Unlike the CIAO, the Deputy CIAO is not located in the Office of the CIO. Organizationally, the CIAO and the Deputy CIAO are within groups under the management of SBA's Chief Operating Officer. Continuity of operations (COOP) for SBA systems is assigned to the CIAO. Physical and operational securities are assigned to the Deputy CIAO. SBA has separate staffs assigned to physical security and information system security with little or no duplication of effort. Both groups work closely in coordinating the Agency's COOP.

4. Critical asset prioritization and protection methodologies.
The IG reported SBA underwent a discovery phase of a Project Matrix Review and findings indicated that the Agency systems do not meet the threshold for a full Project Matrix review.

The Agency used system security plans and a mix of full system risk assessments and GISRA self-assessments to identify its critical systems. SBA had not developed an agency-wide integrated security plan for implementing and integrating its computer security program across all general support systems and major applications.

For disaster recovery and contingency planning purposes, SBA drafted, but had not finalized, a written plan that identifies the sensitivity of SBA systems by the time needed for recovery. The Agency had not determined which mission critical general support systems and major applications must be recovered in the event of a full emergency in which all systems are disabled.

5. Department documented procedures for reporting and sharing vulnerabilities.
In June 2000, SBA and FedCIRC developed a Memorandum of Understanding that requires a quarterly report of security incidents to FedCIRC. The IG reported that the first quarterly report was not submitted until two years later in July 2002. Further, the Agency had seven probes or scans of its Internet router that met FedCIRC's criteria for reporting immediately and did not report them until the July 2002 quarterly report was submitted.

The Administrator delegated reporting of security incidents to the CIO who then further delegated responsibility to the Agency Computer Security Program Manager. The Agency issued the SBA Computer Emergency Response Team (CERT) procedures manual to provide guidance on reporting security incidents to the Agency Computer Security Program Manager who would then report those incidents to FedCIRC.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
In FY 2002, SBA assessed 22 of its 37 systems for risk and assigned a level of risk to them. Twenty two of its 37 systems had an up-to-date security plan. The IG reported that 22 systems had been authorized for processing following certification and accreditation (SBA reported that 24 had been authorized). Fifteen systems were operating without written authorization; although, SBA reports that 16 were operating without written authorization. The IG reported that none of the 37 systems had the costs of their security controls integrated into the life cycle of the system, while SBA reported that five did have controls integrated. Only one of the 37 systems had its security controls tested and evaluated in the last year; although, SBA indicated that two had the security controls tested and evaluated. The IG reported that seven systems had contingency plans and eight systems had contingency plans tested in the past year (SBA reports that seven systems had their contingency plans tested in the past year).

2. Department methods to ensure contractor services are secure.
The IG reported that SBA has a cross servicing agreement with the U.S. Department of Agriculture (USDA) National Finance Center (NFC) for payroll services. The Agency relied upon the USDA IG to perform audit services to ensure that SBA's payroll services were adequately secure and met federal processing standards. In addition, in FY 2002, SBA had

services provided by three contractors. SBA reviewed the security of services of two of these three contractor operations or facilities.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
SBA reported a total of 4,112 employees in FY 2001 and a total of 4,022 employees and contractors in FY 2002. The number and percentage of agency employees including contractors that were reported to receive security training in FY 2001 was 3,906 and 3,411 in FY 2002.

SBA requires all employees to complete annually basic End-User online Computer Security Awareness training (CSAT). In addition to the basic awareness course, SBA maintains three role based CSAT modules for users with additional security duties, which are also mandatory, based on the individual's security role. The additional modules are Functional Program Manager, Designated Security Officer (DSO)/IRM, and System Administrator (SA). SBA requires personnel with full administrative rights to complete the SA computer security training, but highly encourages help-desk, networking, database administrators and application developers to also take SA training.

Two hundred and thirty-one employees had significant security responsibilities in FY 2001 and 231 DSOs and 20 SAs had significant security responsibilities in FY 2002. The number of employees with significant security responsibilities that received specialized training increased from 56 in FY 2001 to 143 DSOs and 78 SAs in FY 2002. The IG indicated that SBA does not offer adequate technical security training at the network or application level for security administrators as was reported in SBA OIG Audit Report Number 2-18, dated May 6, 2002.

2. CIO methods to ensure contractor services are secure.
SBA has a contract to provide mainframe and midrange computing services for its high priority systems. Security personnel within the Agency reviewed computer security at the contractor facility in FY 2002.

3. Agency integration of security and capital planning.
SBA submitted one FY 2003 capital asset plan and justification but without the requisite security information and costs according to the IG. Further, the IG reported that the Agency capital asset plan, justifications, and Exhibit 53 for FY 2004 were not completed and provided to the IG in time for inclusion in its evaluation.

SBA reported that it submitted one FY 2003 capital asset plan and justification and 22 for FY 2004. For FY 2004, SBA reported that security costs were reported for all agency systems on its Exhibit 53. For both FY 2003 and FY 2004, discrepancies still needed to be corrected. Finally, no FY 2003 capital asset plans and justifications were independently validated by the CIO/other appropriate official prior to submittal to OMB, but SBA reported that 22 had been for FY 2004.

Social Security Administration (SSA)

A. General Overview

1. Security funding.
The Agency reports planned FY 2003 funding for IT security of $73.4M. This funding level comprises 8.6% of their total planned IT portfolio of $856M.

2. Number of programs reviewed.
The IG reported that SSA had not identified all of its systems for appropriate review. In FY 2001, SSA completed the certifications and accreditations (C&As) of its sensitive systems. In FY 2002, SSA updated its security program to include one additional system bringing the total to 17 sensitive systems. GISRA requires that Federal agencies review all systems annually, not just "sensitive" systems.

3. Material weaknesses.
SSA did not report any material weaknesses in either FY 2001 or in FY 2002. The Agency did indicate one reportable condition under the Chief Financial Officers Act of 1990, Public Law No. 101-576, to "strengthen controls to protect its information," that did not rise to the level of a material weakness. SSA commented that it has a plan of action to remove the reportable condition, as has been reported in its quarterly Plan of Action and Milestones (POA&M) reports to OMB. However, the IG pointed out that OMB guidance indicates that "…all security weaknesses found during any other review done by, for, or on behalf of the agency, including General Accounting Office (GAO) audits, financial systems audits, and critical infrastructure vulnerability assessments." Based on all IG, GAO, and contractor reports, including vulnerability assessments, the IG indicated that SSA should consider reporting the following additional weaknesses – the need to: 1) improve coordination for continuity of operations plans between the information technology (IT) team and business operations; 2) improve the policy for monitoring and reporting network use, activity, and violations; and 3) apply encryption technology to external sensitive transmissions.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
In FY 2001, an IG recommendation suggested that SSA centralize its security structure and security program. The Agency was compliant with this recommendation and implemented this centralization in FY 2002. SSA established a new Office of the Chief Information Officer (OCIO) at the Deputy Commissioner level and created a Chief Security Officer (CSO) position. The Commissioner of Social Security delegated the responsibility of overseeing systems security issues to the CIO, who reports directly to the Commissioner and Deputy Commissioner. The Office of the CIO also oversees all major IT acquisitions to ensure consistency with the Agency's IT architecture and budget.

The Commissioner established a security performance measure for all senior officials, and established two specific measures of the operational effectiveness of the Agency's information security program for the CIO. The CIO performance measure states, "For FY 2003, no more than 200 workstations will be adversely affected by any security incident, such as a virus. For FY 2004, the goal is no more than 100 workstations." (SSA has over 100,000 workstations.) The performance measure that was added to the Performance Plan/Rating Form for all SSA members of the Senior Executive Service is, "Leads critical infrastructure protection, security measures and other controls necessary to prepare for and mitigate negative consequences."

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Agency conducted annual reviews of security practices and controls as part of the sensitive systems accreditations and certifications. The CIO chairs the Executive-Level Information Technology Advisory Board, which performs annual agency-wide IT planning and prioritization. Through this process, costs, benefits, schedules and life cycle expectations for each selected investment are established and reviewed by the Advisory Board annually and more frequently, as needed.

In addition, in FY 2002, a workgroup on Security in Systems Development Life Cycles (SDLCs), chaired by the Office of Systems Principal Security Officer, developed four standards for SDLCs based on the type of platform, operating environment and system function. The four standards for SDLCs include: 1) legacy mainframe systems, 2) new application systems, 3) Internet systems, and 4) intranet and LAN systems (currently under development). As a result of the new standards, there have been improvements made to the documentation of security requirements within all recently approved system SDLCs.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG reported that SSA integrated its information security program with its critical infrastructure protection (CIP) responsibilities and other security programs. The Executive Internal Control Committee (EIC), comprised of the Deputy Commissioner for SSA (chair), the Deputy Commissioner for Finance, Assessment and Management, and the IG oversees the CIP in SSA. The EIC also provides executive-level oversight for Information Security, Physical Security and Personnel Security. The newly established CSO has policy responsibility for all IT security and the CIO, with the advice of the executive-level investment board, approves budgets for all IT security programs.

4. Critical asset prioritization and protection methodologies.
SSA reported, and the IG concurred, that the Project Matrix Step I Review was completed in FY 2001. The Agency contracted to have vulnerability assessments, including risk assessments, performed on the critical assets identified in its Project Matrix Review. Most of the vulnerability assessments were completed, according to the IG, and SSA indicated that only two remain to be completed-one was in process, and one is scheduled to be done in FY

2003. With the assistance of the Critical Infrastructure Assurance Office (CIAO) and the SSA Inspector General, SSA has begun Project Matrix Step II Reviews.

5. Department documented procedures for reporting and sharing vulnerabilities.
SSA indicated that incident reporting procedures are contained within the SSA Security Handbook and are a focus of ongoing employee awareness training. In addition, the Agency stated that all attempts at security intrusion are closely monitored, recorded and reported to FedCIRC. The SSA technical staff holds a daily telephone conference with FedCIRC technical staff and routinely exchange current information regarding attempted intrusions, viruses and other types of security threats. Typically, SSA reports security incidents immediately to the Agency-wide help desk. Once the incident has been confirmed, SSA reports it to FedCIRC about 30 minutes later. The Office of Systems Security Operations Management also provides FedCIRC with a quarterly summary report. In addition, SSA and FedCIRC are working on finalizing a Memorandum of Agreement that will delineate specific response times for the reporting of security incidents.

In addition to reporting security incidents to FedCIRC, SSA reported that it confirms that patches have been tested and installed in a timely manner through expedited change control and testing processes tracked by the "Intrusion Protection Team".

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
Agency program officials maintain an up-to-date security plan for each system supporting the operations under their control. Annual updates, including certifying that adequate controls exist within the sensitive systems or assets, are made for security plans of all sensitive systems. However, the IG noted that its reviews of the certifications and accreditations that were completed for these systems indicated that few specific system weaknesses were reported even though references were made in the reports indicating that findings and recommendations exist.

SSA reported that 100 percent of its 17 sensitive systems had been assessed for risk, had a level of risk assigned after a risk assessment has been conducted, and that all 17 of these systems had an up-to-date security plan. All of the 17 sensitive systems had been authorized for processing following certification and accreditation and no systems are operating without written authorization. Further, the Agency reported that 100 percent of the 17 sensitive systems had the costs of their security controls integrated into the life cycle of the system; had security controls tested and evaluated in the last year; and had a contingency plan. Ninety four percent of the 17 sensitive systems (or 16 of the 17 systems) had their contingency plans tested in the past year.

2. Department methods to ensure contractor services are secure.
The IG reported that in order to ensure that contractor- or Government-provided services are adequately secure and meet GISRA requirements, OMB policy, NIST guidelines, and Agency policy, SSA program officials revised prior contract language. This language now

requires that contractors ensure their staffs conform to the security requirements for federal employees. The IG noted that since the inception of the new contract language, SSA performed limited physical reviews of the contractors. SSA reported that of 75 contractor or other agency operations or facilities, in FY 2002, 44 contractor or other agency operations or facilities were reviewed.

SSA commented that most of its connections are to other government organizations and facilities (65 out of the total of 75). Some of the 44 reviews conducted in FY 2002 include other Federal agencies where there is an ongoing relationship between SSA security organizations and the security organizations of the other agency. Periodic reviews and reports are done with state agencies and those Federal agencies with which there is less frequent contact.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
Because SSA's missions and systems are relatively homogeneous, the Agency has been able to have strong central control over all IT functions, especially in the area of information security. SSA reported that there had been a strong emphasis over a long period of time on technical standardization. Component organizations within SSA are permitted to use only a limited number of standard technical approaches for the security of their application systems. All mission critical systems and systems required for their support go through an annual risk assessment and re-certification process.

In addition to having policies and procedures that are monitored for compliance, SSA tests and evaluates the effectiveness of its security controls through a combination of continuous network monitoring, "red teams," vulnerability analyses and penetration testing of its internal and external telecommunications networks, platforms and individual application systems. These tests and evaluations are in addition to the testing performed by the IG.

SSA indicated that during FY 2001, it conducted an above average amount of training to ensure that all employees with significant security responsibilities met the requirements for a basic security skill set. (At a minimum, all employees and contractors receive basic security awareness training. In addition, each security officer must receive 16 hours of security training each year to maintain his or her skill level.) In FY 2001, 342 employees out of a total of 66,000 employees including contractors, were identified by SSA as having significant security responsibilities and all 342 employees received specialized training. In FY 2002, 428 employees were identified as having significant security responsibilities out of a total of 66,000 employees including contractors. The FY 2002 specialized training for these 428 employees consisted of an average of 3.4 courses per employee. SSA noted that in FY 2002, the level of training has been at a more typical "maintenance level". SSA reported funding FY 2001 training at $400 thousand and at approximately $255 thousand in FY 2002, which reflects this "maintenance level" of training.

2. CIO methods to ensure contractor services are secure.

See C.2. In addition, the Agency designated to the CSO the responsibility for ensuring that services provided by contractors or another agency are adequately secure and meet all applicable requirements. The IG reported that the current mechanism for ensuring contractor compliance is a contract template.

3. Agency integration of security and capital planning.
The IG reported that the CIO's key involvement in the Agency's capital planning and investment control process ensures the CIO's ability to integrate security into the IT budget. The Agency reported that it submitted to OMB 18 capital asset plans and justifications for FY 2003 and 21 for FY 2004. All of them contained the requisite security information and costs and security costs were reported for all agency systems on the agency's exhibit 53, according to SSA. The IG confirmed SSA's indication that this information has been reported.

Department of State (State)

A. General Overview

1. Security funding.
The Department of State reports planned FY 2003 funding for IT security and critical infrastructure protection of $191.4M. This funding level comprises 22% of their total planned IT portfolio of $852M.

2. Number of programs reviewed.
The Department reported a total of 22 programs, all of which were reviewed in FY 2002. The total number of agency systems reported by the Department was 306, of which State indicated they reviewed 30 systems. GISRA requires Federal agencies to review all systems annually. In addition, the Department reviewed 161 of its 344 components (30 Bureaus, 256 Posts, and 58 Field Offices).

The Department used the NIST *Guidelines and Framework for Self-Assessment* to review all major corporate applications. State expects full utilization of this tool in FY 2003.

3. Material weaknesses.
In FY 2001, the IG identified a material weakness in the Department's lack of certification and accreditation of its information systems. To address this key deficiency, the Department developed a strategy aimed at implementing the National Information Assurance Certification and Accreditation Process (NIACAP) across the Department, including quick certification and accreditation of all Department systems, networks, applications, domains, and sites. However, the IG reported that the Department had not developed a timetable for certification and accreditation (C&A) of all systems. According to an IG survey questionnaire, only 15 percent of the Department's systems had security plans.

The IG found a significant weakness in information security management at overseas missions. Specifically, the IG determined that the information systems security officers (ISSO) generally were not performing all the requisite duties of the position. None of the 11 missions visited by the IG had developed information security plans and the IG found deficiencies in management, and technical and operational controls.

The IG reported that State had made some progress in assessing information security at missions and bureaus as part of its implementation of OpenNet Plus, the Department's program to provide worldwide desktop Internet access to its employees. Missions must show that they comply with existing security standards prior to receiving Internet services from OpenNet Plus. As of September 3, 2002, 20 bureaus and 84 missions had met the requirements of independent verification and validation (IV&V) of their respective IT infrastructures indicating compliance with the Department's IT security configuration and have subsequently been connected to OpenNet Plus.

Additional material weaknesses identified by the IG include: lack of information security performance measures to support strategic goals; weaknesses in the critical infrastructure protection program that have not been addressed; and Departmental management of information security as identified in three different information management programs: Munitions Controls Systems, Classified Connectivity Program; and Central Financial Management System.

In FY 2001, State reported no material weaknesses, but indicated that it corrected four material weaknesses last year. In FY 2002, the Department reported three material weaknesses. The Department had its 2001 financial statements audited by an independent auditor at the direction of the IG. This independent auditor cited a "material weakness" for "the Department's information systems security for networks in domestic operations."

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.

The IG reported that State had not implemented information security performance measures to support its strategic goals. While IT security performance measures were in the process of being phased in, State's Under Secretary of Management had reevaluated the roles and responsibilities of program officials with security authority and instituted changes to agency-specific roles in order to comply with GISRA. The Department reported that these changes clearly and unambiguously set forth responsibilities and authorities for the agency CIO, Diplomatic Security (DS), and program officials. The System Security Program for the Department has been implemented through the publication of policy in the form of Foreign Affairs Handbooks and Manuals, telegrams to the overseas posts, Department Notices to the domestic bureaus, security listservs, and newsletters. New security requirements were added to budget submissions that require the approval of the CIO and the Chief Financial Officer (CFO).

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported on a number of material weaknesses in the area of lack of security plans, lack of performance measures and system certification and accreditations, as well as deficiencies in other areas that indicate that the security plan is not practiced throughout the life cycle of each system.

In response to the IG's reporting that the Department had not developed information security performance measures to support its strategic goals, the CIO issued the Department's FY 2003 Information Assurance Performance Measures Plan. In addition, the CIO requested that all bureaus and missions implement procedures for collecting and submitting data in accordance with the plan.

In the first quarter of FY 2002, the Department reported that two functional Bureaus with significant security objectives, Diplomatic Security and Information Resource Management, created performance measures. The Department announced a phased approach for implementation of specific IT security performance measures that will be used throughout FY 2003 for data collection reporting.

The Department further reported that the Secretary works through the Deputy Secretary, the Under Secretary for Management, the CIO, and the Assistant Secretary for Diplomatic Security to ensure the agency information security plan is practiced throughout the life cycle of its systems. During FY 2002, the Under Secretary for Management mandated the Department-wide implementation of the National Information Assurance Certification and Accreditation Process (NIACAP) in a timely and efficient manner. The Under Secretary approved the DS and IRM roadmap for implementing this plan.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
The IG indicated that the Department had not addressed weaknesses in its critical infrastructure protection program. As discussed in its June 2001 report on *Critical Infrastructure Protection: The Department Can Enhance Its International Leadership and Its Own Cyber Security*, the IG highlighted a number of areas that State still needed to address. These included assessing the vulnerability of the Department's foreign operations to cyber-based disruptions; scheduling and conducting security control evaluations of all minimum-essential cyber infrastructures at least once every three years; ensuring that subsequent critical infrastructure protection plans and vulnerability assessments address minimum-essential interagency infrastructure vulnerabilities; and testing security controls. The IG indicated that in part, these areas had not been addressed because State is in the process of revising its critical infrastructure planning.

In February 2002, the Under Secretary for Management established a formal Department-wide Critical Infrastructure Protection (CIP) program to be managed and resource loaded over a multi-year planning period that is aligned with the Department's budget and planning process to achieve their CIP objectives for domestic and overseas operations. The Under Secretary assigned lead responsibility for this activity and also for the formulation and

execution of the Department-wide CIP Program Plan to the Assistant Secretary for Resource Management. A Critical Infrastructure Protection Governance Board comprised of Assistant Secretaries and equivalent was established. This Board oversees the CIP Program and also participates in the formulation and execution of the Department-wide CIP program plan to achieve the CIP objectives of the Department of State's domestic and overseas operations.

A CIP working group, which reports to the Governance board, addresses and coordinates aspects of the Department's critical infrastructure activities. The working group is pursuing requirements (business and funding for Continuity of Operations Plans (COOP) and Continuity of Government (COG) across Department Offices. The working group is also coordinating the writing of an updated enterprise-wide critical infrastructure plan, to be authored by the Bureau of Information Resource Management (IRM) and vetted through the CIP Governance Board. As part of these responsibilities, the Working Group is working closely with IRM to identify and establish alternate operating sites, and to remediate previously identified Information Technology vulnerabilities.

The Department's contingency planning initiative ensures that Bureaus, overseas posts, and affiliate organizations can continue their respective mission or business at all times and minimize the impact of disasters which threaten life, property and the Department's IT infrastructure. Contingency planning is a key requirement of certification and accreditation, and a standard approach is being pursued at the infrastructure, domain, site and system level. A complementary effort, Emergency Action Plans (EAP), addresses operational and physical security at overseas locations. The Department fields crisis management teams that validate the approach and plans.

4. Critical asset prioritization and protection methodologies.
Overall, the IG found that the Department had not addressed weaknesses in its critical infrastructure protection program, but did not specifically comment on critical asset prioritization and protection methodologies.

State reported that the Department's CIP Governance Board (CIPGB) had begun the first phase of a Project Matrix review of identifying all assets nation-wide. The CIP Working Group is actively pursuing, on a bureau-by-bureau basis, the identification of assets that contribute to the essential operations of the Department. The Department expects an overlap with Project Matrix in some areas, where specific assets will be considered critical in both agency and national scope.

State is working closely with the Critical Information Assurance Office (CIAO) to resolve classification, handling and access issues which currently exist. When complete, the Department's assets will be listed and categorized according to business function and criticality.

5. Department documented procedures for reporting and sharing vulnerabilities.
The IG did not specifically address this area.

The Department reported that as part of its Incident Handling Program, the Computer Incident Response Team (CIRT) serves as the focal point for reporting computer security events and incidents on automated information systems utilized by the Department. Established in 1998, CIRT is also the primary conduit for passing incident-related information to law enforcement organizations both within and outside the Department as well as sharing information with other incident handling entities. CIRT developed detailed operating procedures governing the review, analysis, and resolution of events reported by the Department's Network Intrusion Detection Center, Regional Security Officers, Information System Security Officers, system managers and IT users. In addition, CIRT established procedures for assisting law enforcement with criminal investigations and prosecutions. CIRT determines whether an event is an operational error (e.g., improper software configuration) and if the event/incident could damage or disrupt the Department's networks. Operational matters are referred to IRM for resolution while other incidents are reported to external authorities such as FedCIRC and the NIPC for data correlation, pattern recognition, and additional analysis. Viruses are reported to the Department's Virus Incident Response Team (VIRT). CIRT's performance goal is to resolve most of its cases (90%) within 10 days or less.

In addition, the Cyber-Threat Analysis Cell (CTAC) supports the Department's information sharing program by maintaining a comprehensive database to identify common attackers and methods, analyze long-term trends, and promote increased communication between operational and security oriented offices within the Department and federal community.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reported that the Department had been slow in addressing the information security deficiencies identified in the IG FY 2001 GISRA report. According to the IG, only ten percent of systems were reported to have security plans, and only five percent were reported to have been certified and accredited. The IG identified additional weaknesses in the Department's management of information security in its reports on three different information management programs: Munitions Controls Systems, Classified Connectivity Program (CCP), and Central Financial Management System (CFMS).

The Department indicated it has developed several initiatives specifically tailored to mitigate risk on IT operations across its enterprise. In addition, independent evaluation and penetration testing is performed on an annual basis to test current security posture and redress weaknesses.

2. Department methods to ensure contractor services are secure.
The IG did not specifically comment on this area.

The Department manages both classified and Sensitive But Unclassified (SBU) contracts in accordance with Federal Acquisition Regulation, and as applicable, with the Foreign Affairs Manual (FAM). In accordance with the National Industrial Security Program, established by

Executive Order (E.O.) 12829, contracting firms and their employees must be cleared prior to accessing classified information. Contracting firms are required to comply with the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M, for the protection of classified information. NISPOM prescribes the standards for protecting classified information possessed by contractors and provides information system security requirements. The Defense Security Service (DSS) must approve systems housed at contractors' corporate locations. DSS clears the contracting firms and their employees and provides oversight for the firms' protection of classified information and systems.

For SBU contracts, the Department reviews contracts provided by various Bureaus. If investigation and adjudication are warranted for contractor personnel by virtue of their duties and responsibilities, the security requirements are provided to the Contracting Officer's Representative (COR) for inclusion in the contract. In addition, a clause is required for use "in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development or operation of a system of records using commercial information technology services and support services."

In FY 2001, State reported a total of 16 contractor operations or facilities, nine of which were reviewed. In FY 2002, State reports having reviewed 16 of its 23 contractor operations or facilities.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.

In its February 2002 report on State's Classified Connectivity Program (CCP), a project to implement classified processing capability at overseas missions, the IG reported that the Department had not developed a definitive strategy for managing the security risks of its CCP deployments. At overseas missions, the IG found significant weaknesses in information security management. Generally, the information systems security officers (ISSOs) were not performing all the requisite duties of their positions. Also, none of the 11 missions that the IG visited had developed information security systems plans. In addition, the IG found a number of information security vulnerabilities through its review of key information management programs and the lack of certification and accreditation was noted to be a significant concern.

The IG did not specifically address the area of training employees in IT security. However, the Department reported that in FY 2002 approximately 2,800 employees had been identified as having significant security responsibilities and that all of them have received specialized training. State indicated that security "awareness" is required of all employees and that as of the close of the FY 2002 third quarter, 9,665 employees out of a total of 31,975 agency employees, including contractors, had received specialized "awareness" briefings, including users of OpenNet Plus.

State indicated that only some of all known security weaknesses are addressed by the Department's Plans of Action and Milestone (POA&M) reports. POA&Ms were not

currently integrated as a complete and comprehensive, single-source for eliminating known and documented vulnerabilities for programs and systems within the Department. Additionally, State indicated that it has taken a phased approach to performance measurement and has required that all bureau executive directors implement performance measures within their respective bureaus in FY 2003.

2. CIO methods to ensure contractor services are secure.
See C.2.

3. Agency integration of security and capital planning.
The IG did not specifically address this area.

The Department reported that they have fully integrated security into their capital planning and investment control process. The IT Investment Portfolio System (I-TIPS) used by the Department supports the activities of the IT Program Board (ITPB) whose purpose is to assess needs and requirements for technology, and assure available resources are effectively and efficiently used in support of the Department's mission. The review process for the ITPB includes an analysis by both the Technical Review Advisory Group (TRAG) and the Management Review Advisory Group (MRAG).

United States Agency for International Development (USAID)

A. General Overview

1. Security funding.
The Agency reports planned FY 2003 funding for IT security and critical infrastructure protection of $21M. This funding level comprises 21% of their total planned IT portfolio of $99M.

2. Number of programs reviewed.
In FY 2002, USAID reported a total of six programs, of which four had been reviewed. The programs that had not been reviewed were in the early phases of the life cycle. Work on them includes discussion of security issues appropriate to their life cycle phase, with many of the systems' security issues being actively addressed in the IT infrastructure program. USAID believes that the Agency is in compliance with security requirements on these systems given their stage of development.

In FY 2001, the Agency reported a total of 8 systems, of which all 8 had been reviewed. In FY 2002, USAID indicated a total of 89 systems, of which 85 had been reviewed. The Agency noted that the increase in the number of systems from FY 2001 to FY 2002 was a result of treating 81 separately managed segments of the General Support System (GSS) as separate systems in FY 2002, but not in FY 2001. The four systems not reviewed in FY 2002 are GSS segments that did not receive a formal risk assessment, but did receive oversight of

managerial controls, regular vulnerability scans of technical vulnerabilities, and follow-up on technical vulnerabilities that had been identified.

USAID used the NIST self-assessment guide to assist in these reviews. In addition, the Agency supplemented USAID-specific methodology to add quantitative risk assessment allowing cost/benefit assessment of potential controls at the enterprise level, as well as at security-perimeter levels.

3. Material weaknesses.
The IG identified significant weaknesses in USAID's management of information technology resources, including (1) computer security and (2) information resources management processes. Specifically, IG reports showed that USAID did not have adequate computer security controls in place to mitigate the risks to critical information systems. The Agency needs to strengthen logical access controls and eliminate conflicting accounting roles in its financial management processing. Further, the IG recommended that USAID conduct certifications and accreditations (C&A) on all mission-critical network and financial management systems. This includes conducting a risk assessment, incorporating detailed recovery and testing procedures in a contingency plan, and developing a security plan as required by federal standards. The Agency concurred with the IG in identifying its computer security program as a material weakness.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
In FY 2001, the IG reported that the Agency had responded to the GISRA requirement to develop information security policies, procedures and controls. However, the IG reported that some of USAID's policies and procedures did not adequately incorporate security into information technology (IT) processes as required by GISRA, such as the Agency's capital planning and investment process, enterprise architecture process, and contractor provided services.

At the end of FY 2001, USAID had become largely compliant in documenting basic Responsibilities and Authorities (R&A). The Agency had developed basic content for training key security officials to explain their R&As and an Agency ISSO was in place and aware of the R&As. In FY 2002, USAID updated and improved documented policies, such as the R&As, and the CIO now reports directly to the Administrator. The ISSO now reports directly to the Office of the Chief Information Officer. Responsibility and authority for security has been explicitly delegated to overseas posts (Director and ISSO). The Agency is working on reducing reliance of decentralized ISSOs by centralizing key security responsibility and authority via remote monitoring and administration to centralize R&A.

In addition, IT investment decisions about the headquarters infrastructure within the Management Bureau, international communications infrastructure, and most corporate application servers within overseas missions cannot be made without review by and concurrence of the CIO. However, some components may, such as the IG and Office of

Foreign Disaster Assistance (OFDA), have special authority to make independent infrastructure investments because of the need for independence (OIG) or rapid response capability (OFDA). Overseas posts have limited IT investment authority independent of the CIO's review or concurrence to provide desktops and network servers for their local staff, for example, or to develop small applications for local use. The latter has often resulted in lack of coordination and capital budgeting. To address these concerns, the CIO and ISSO are encouraging a standardized life cycle, enhancing security reviews of these systems, and incorporating reviews in capital budgeting decisions.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The IG reported that the Agency had not established effective performance measures and implemented corrective actions as a result of USAID security team's evaluations. This has contributed to deficiencies that expose USAID to unacceptable risks that resources will not be adequately protected. The Agency and IG are in concurrence that this is largely due to lack of implementation of a centralized function that has oversight and ensures that USAID meets security requirements.

The Agency began work to improve this situation. USAID developed and deployed a tool to assist overseas posts to create a security plan consistent with the overall Agency plan. As a result, in FY 2002, of its 75 missions, 21 draft security plans for overseas posts were submitted by the end of the IG fieldwork audit (July 17, 2002) and three plans had been finalized. USAID intends to follow up to ensure that the remaining 51 missions adequately develop their security plans.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
While USAID has specialized groups performing components of security, the Agency reports that their work is integrated and does not overlap. The director of the relevant offices coordinates their efforts to avoid duplication. Physical security, personnel security, and national security information security are managed by USAID's Office of Security. Continuity of Operations Planning (COOP) is coordinated by the Agency's Administrative Management Services (AMS) Office. Information Security (non-national security) is handled by the CIO and ISSO.

In FY 2001, USAID did not develop a critical infrastructure plan (CIP). The Agency maintains that the Department of State has responsibility for completing the plan because of its designation as lead agency for foreign affairs. USAID reported that the State Department had not assigned any special CIP responsibilities to the Agency. Further, while USAID's IT infrastructure is critical to the operation of USAID, the Agency reported it did not necessarily meet the level of criticality defined by the CIP program.

4. Critical asset prioritization and protection methodologies.
USAID did not undergo a Project Matrix review to identify the interdependencies between its critical assets (its IT infrastructure) and services provided by others. Instead, the Agency identifies critical assets through their normal technology architecture exercises. The

interdependencies consist largely of reliance on a number of private and public sources to provide voice and data telecommunications connectivity among headquarters, USAID overseas missions, and USAID IT service providers. The primary step the Agency has taken to mitigate the risk created by these dependencies is to provide redundant communications links between sites.

In August 2001, USAID developed its current list of mission critical systems for the GISRA review. The list included eight systems, three of which are operated by other agencies. However, in April 2002, USAID designated four of its eight mission-critical systems as major and the other four as minor systems and outlined its plan of what security requirements would be applied to major and minor mission-critical systems. The Agency will apply the following security requirements to its major systems: assign responsibility for security; prepare a security plan that meets OMB Circular A-130 requirements; conduct a review of application controls at least every three years; authorize processing based on the review conducted; prepare an adequate Continuity of Operations Plan (COOP) and disaster recovery plan; conduct a quantitative risk assessment defining risk in terms of dollars and identifying opportunities to increase security at high benefit-cost. For its minor systems, USAID will prepare an adequate COOP and disaster recovery plan and conduct a quantitative risk assessment defining risk in terms of dollars and identifying opportunities to increase security at high benefit-cost.

5. Department documented procedures for reporting and sharing vulnerabilities.
Last year, the IG reported that USAID had not fully implemented an incident response and reporting capability. USAID published policy guidance that instructs Agency personnel on how to report a security incident. However, the incident response reporting had not been fully implemented. Subsequent to the report last year, USAID issued a mandatory reference to its Automated Directives System (ADS) addressing how to report an information security incident. The Agency was revising its USAID *Incident Response Capability Handbook Coordinating Draft*. The new procedure includes the requirement that security incidents be described in reports submitted to USAID's ISSO. The ISSO in turn is required to notify the IG about information security incidents involving any apparent violation of laws, rules or regulations; and submit computer security reports on behalf of USAID to FedCIRC.

During an ongoing review of the Agency's general controls, the IG determined that incident response procedures at two of the three missions reviewed to date were not completed. As a result, those missions may not be able to contain and repair damage from security incidents and prevent future damage.

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
In FY 2002, USAID reported that 89 systems had been assessed for risk. For 81 of the 82 General Support System (GSS) segments (included in the 89 systems), the assessments were largely limited to managerial and technical controls based on review of mission security plans, and remote technical vulnerability scans. All 89 systems had been assigned a level of

risk. Sixty-three systems had an up-to-date security plan. All 89 systems had been authorized for processing following certification and accreditation. Twenty of the 89 systems had the costs of their security controls integrated into the life-cycle of the system. Seventy-five of the 89 systems had their security controls tested and evaluated in the last year. Thirty-eight of the 89 systems had a contingency plan.

2. Department methods to ensure contractor services are secure.
In FY 2001, the IG reported that USAID did not have a documented methodology to evaluate if contractor-provided services were meeting security requirements. At the conclusion of its FY 2002 fieldwork, the IG was told by the Agency that its CIO is working with the Agency's Office of Procurement (using NIST guidelines) to develop appropriate information security clauses for USAID contracts. In addition, USAID has three mission critical information systems that are managed by outside contractors. The Agency reported that there are security plans for all three of these systems.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
In FY 2001, the IG reported that deficiencies in security policies and procedures existed because USAID's security program lacked a strong centralized security function to ensure that its policies and procedures addressed key components of security management. In response, the Agency implemented changes that included the CIO reporting directly to the Administrator and the ISSO reporting directly to the CIO. USAID's guidance on information systems security states that the Assistant Administrator, Bureau for Management (AA/M) serves as the CIO. The CIO may delegate day-to-day supervisions of the ISSO function to their Deputy. However, the ISSO will maintain a direct reporting channel to the CIO in the event that it is needed to coordinate or gain adequate support for the information security program.

In FY 2001, the IG report indicated that while USAID provided its employees and headquarters-based contractors with security awareness training, it needed to provide specific training to key personnel to carry out their security responsibilities. The Agency also needed to provide annual refresher briefings to all employees and for seven of eight overseas missions that the IG visited last year. In FY 2002, USAID developed and began to implement a security awareness training program utilizing compact disks and web-based applications with an automated tracking system. The Agency also provided security responsibility training to its ISSOs and M/IRM security staff; risk vulnerability, management and awareness training to ISSOs; and training on security vulnerabilities and mitigation for the Mission Accounting and Control System to new entry controller trainees.

The IG raised the following concerns about USAID's security training implementation approach: (1) at the conclusion of the IG fieldwork in July 2002, while the tracking system for the training program could identify who took the training, it did not identify when they took it, nor could USAID match those taking the training against a list of users required to take it; (2) the Agency's web page does not provide a direct link from the home page for

users to access the ISS training and users therefore, must search the website to find the training; and (3) while USAID reported that it would identify the positions with key security roles and responsibilities, it has not identified the individuals in these roles and therefore, cannot determine if all employees with significant security responsibilities receive the specialized training. Because the Agency is in the process of implementing IG recommendations to improve the security training program, the IG reserved further comment until those recommendations have been fully implemented.

2. CIO methods to ensure contractor services are secure.
USAID reported a total of 82 contractor operations or facilities in FY 2001and FY 2002. In FY 2001 and FY 2002, 77 contractor operations or facilities were reviewed only for managerial and technical controls. Only two of the contractor operations or facilities were reviewed for all controls in both fiscal years.

USAID has three mission critical information systems, which are managed by outside contractors. USAID reports that these three systems had not been reviewed as the Agency has had difficulty obtaining adequate information from its providers. For one of these three systems, the IG reported in a March 2002 audit report that the Agency had not prepared a security plan for that system.

At the end of FY 2001, the CIO did not have a cost effective strategy to oversee program officials' reviews of contractors. In FY 2002, an IG audit of USAID's overseas posts indicated over-reliance on foreign nationals for whom adequate background checks, supervision, and separation of duties are performed. The Agency's CIO and ISSO subsequently developed a strategy to resolve this concern and lack of oversight by program officials based on using centralized remote administration of decentralized security assets. In addition, USAID's CIO is working with the Agency's Office of Procurement to develop appropriate information security clauses for USAID contracts.

3. Agency integration of security and capital planning.
In FY 2002, USAID redesigned its overall governance structure for the acquisition and management of IT that served to elevate the entire IT investment process. The Agency created the Business Transformation Executive Committee (BTEC) to provide Agency-wide leadership for initiatives and investments to transform its business systems and organizational performance. BTEC, staffed with senior members of Agency management, will assist in the development of policies and procedures related to IT governance. USAID reported that it has consulted with various project managers in the implementation of OMB Circulars A-11, Exhibit 300 and Exhibit 53 that pertain to the subject of incorporating security considerations in the investment planning process. The Agency also reported that several USAID project managers received training from OMB for capital asset planning. In addition, USAID developed a strategy to reduce the level of security investment in decentralized overseas posts and developed a detailed analysis of central security costs in the central OE budget.

Department of Veterans Affairs (VA)

A. General Overview

1. Security funding.
The Department of Veterans Affairs reports planned FY 2003 funding for IT security of $124.8M. This funding level comprises 8.8% of their total planned IT portfolio of $1.42B.

2. Number of programs reviewed.
The Department is comprised of five major organizational components or programs. Of these five programs, the FY 2001 report identified 995 systems with all systems reviewed. The FY 2002 report identified a 14% reduction in the total number of Department systems from 995 to 851 with all of the 851 systems reported as reviewed.

The IG reported unreliable information in the web-based survey data concerning completed security remediation efforts and recommended that the Department establish a verification process to validate input to the database to assure its accuracy.

The Department used a web-enabled survey, modeled after the NIST Special Publication 800-26, Security Self-Awareness Guide for Information Technology Systems, to collect information from the Department's numerous geographic locations. Additionally, Department security directives, NIST special publications, and GAO's Financial Information Systems Control Audit Manual text references were included as links to each applicable question. An analysis of the results of the FY 2002 GISRA survey indicated that the Department self-reported 13,951 deficiencies for systems and major applications.

3. Material weaknesses.
The Department and IG agreed that IT system security had been, and continues to be, a material weakness. The IG recommended that more effective Department-wide security management, oversight, and control over its systems and data would enhance its IT security posture and move towards correction of this material weakness.

B. Responsibilities of the Agency Head

1. Measures of performance used by the agency to clearly set forth the Security Act's responsibilities and authorities for the agency CIO and program officials.
The Secretary continued to take action to effectively integrate IT security into all aspects of Department operations. The Department established the Office of Cyber Security (OCS) and the Office of Assistant Secretary for Operations, Security, and Preparedness to facilitate oversight and implementation of necessary physical and electronic security remediation efforts. The Secretary also issued a directive that intends to centralize all IT functions under the CIO.

The OCS routinely generates GISRA information in the form of performance measurements associated with FISCAM security controls. These FISCAM performance measurements are being generated for each system/major application and updated to reflect POA&M

remediation activities. The CIO and security personnel's opportunity to provide effective oversight, to ensure guidance is uniformly interpreted, and identify those projects and systems wherein managers have failed to take appropriate actions to effectively implement the Department's Security Program and/or remediate identified IT security weaknesses on a timely basis is enhanced by these performance measurements.

The Secretary mandated that the CIO provide a conceptual framework of the new centralized command structure. This will afford the Secretary a direct management interface for all IT issues. This new management focus will allow the organizational components to make IT investment decisions in consultation with, but not necessarily dependent upon, the concurrence of the Department CIO.

2. Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.
The Secretary delegated responsibility to the Department CIO to ensure that the system security plans are up-to-date and practiced throughout the life cycle of each IT asset. The IG reported that the Department does not have a Systems Development Life Cycle (SDLC) for all systems. The older legacy systems do not have properly documented SDLCs. The Department reported that risk assessments will be conducted on legacy systems to determine what security controls are necessary.

The IT Capital Investment Board requires inclusion of life cycle development and has required system security be included in the decision making process. The Department had not developed specific performance measures to address the above listed security issue areas.

3. Integration of information technology, critical infrastructure protection, physical, and operational security programs.
Each of the Administrations has a CIO and support staff that oversees the activities within its Administration. With the Secretary's planned centralization of the IT program under the Department CIO, the IG expects some streamlining of IT security operation across the Department that could lead to elimination of some duplication of effort within the individual Administrations.

The Department began to develop a plan for integrating its information security plan with its Critical Infrastructure Program (CIP). The Office of Cyber Security (OCS) has assumed responsibility for the IT security issues associated with CIP. The Department aligned responsibilities for protection of its non-IT physical infrastructure in the newly-established Office of Operations, Security, and Preparedness (OSP).

4. Critical asset prioritization and protection methodologies.
The Department did not undergo a Project Matrix review. The Department developed a Critical Infrastructure Protection Plan (CIPP) assessment process identifying risks associated with cyber and physical vulnerabilities. The CIPP was developed in 1998 and had not been updated to include current milestones. Based on the IG findings, the plan had not been effectively implemented to protect the Department's cyber and physical assets. The

Department reported that OCS will ensure all future critical infrastructure-related information collected will meet Project Matrix criteria.

5. Department documented procedures for reporting and sharing vulnerabilities.
The Department established and centralized all component incident response capabilities into a single Critical Incident Response Capability (VA CIRC). The IG determined that some of the Department facilities are not reporting incidents to CIRC. To improve on reporting process, the OCS entered into an agreement where all Department elements will be reporting through one vendor and that vendor will report to FedCIRC. The Department indicated that VA CIRC is supplying incident information to OCS, quarterly summary reports to FedCIRC, and is responding directly to FedCIRC inquiries. The CIRC, in concert with facility Information Security Officers (ISOs), coordinates the incident with law enforcement authorities and notifies OIG as appropriate.

For FY 2002, the VA CIRC reported the assistance of nine incidents with external law enforcement. The CIO reported that 10,608 incidents were reported externally to FedCIRC or law enforcement. This number represents a significant increase over FY 2001 reported incidents (1,165).

C. Responsibilities of Agency Program Officials

1. Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.
The IG reported that the Department had not effectively implemented planned security measures and had not assured compliance with established policies, procedures, and control requirements. Also, according to the IG, "the Department's data reported on completed security remediation efforts was not reliable." The database contained information that erroneously reported completed security remediation efforts in areas that the IG vulnerability assessments and penetration testing showed were not corrected. The IG recommended that the Department establish a verification process to validate input to the database to assure its accuracy.

The Office of Cyber Security (OCS) revised the Department's Information Security Plan to update the security policies, procedures, and technical standards for developing risk-based security assessments. This revision also improved the monitoring and testing of systems controls. The Department indicated that it completed risk assessments and identified needed security remediation efforts.

According to the information provided by the CIO, 472 systems (55%) had been assessed for risk and 542 (64%) had been assigned a level of risk. Thirty-one percent of the systems (262) had been certified and accredited and 581 had up-to-date security plans. The IG report did not include an assessment of the performance data presented by the Department; however, security assessments involving major systems indicated that the Department had not made sufficient progress to establish necessary security controls to proactively identify and prevent information security related risks and implement corrective action.

2. Department methods to ensure contractor services are secure.
Although the Department does not routinely require audit or inspection of contractor IT operations or facilities, the Department uses several mechanisms to ensure that contractor-provided services or services provided by another agency are adequately secure. Of the 114 contractor operation or facilities utilized by the Department, 22 had been reviewed. Minimum background investigations are required for outside agency personnel who are afforded access to sensitive Department information and/or IT assets. This investigation is required prior to performance of work under such a contract. Additionally, specific language referencing information security requirements is included in each contract award. Department mandates are included in contractual language to ensure the continued security of Department IT assets. The IG did not include the review of contractor provided services but did concur that the Department had taken various actions to ensure that contractor provided services are adequately secure.

D. Responsibilities of Agency Chief Information Officers

1. Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees.
The IG found that a computer based security awareness training program had been created; however, their results indicated that there are employees who had still not received initial or annual IT security related training. The Department advised that the estimated 230,000 full-time and part-time employees and contractors receive orientation, continuing education and 'role-specific' security training as required by law and policy. Of the 593 employees with significant security responsibilities, the Department reported that it is unknown how many received specialized security training.

The OCS was developing a program for certification of Information Security Officers to include passing the Certified Information Systems Security Professional (CISSP) examination. The OCS has sponsored CISSP training, and strongly encourages all security personnel to obtain this certification, as well as other industry recognized security-related certifications, but will not require individuals to pass the CISSP examination as part of the CSPP credentialing process for an ISO.

2. CIO methods to ensure contractor services are secure.
The Department does not routinely require audit or inspection of contractor IT operations and/or facilities. The Department reported that several effective mechanisms are used to ensure contractor provided services or services provided by another agency are adequately secure. There are no reported contractor operations or facilities.

3. Agency integration of security and capital planning.
The Department reported that security is fully integrated into the Agency's IT capital planning and investment control process, including each of the functional, technical, and strategic review phases. The Department reported that every FY 2003 IT capital investment proposal forwarded to OMB for review addressed security. The CIO also reported that the $70M increase in IT security budget requirements from FY 2002 to FY 2003 was not attributable to new budget requirements or proposed additional IT security spending, but

rather, represented increased Department focus on more accurately compiling those costs associated with IT security by major IT project, and integrating those costs into the Department's capital planning and investment control process.