Office of Management and Budget

FY 2001 Report to Congress on Federal Government Information Security Reform

TABLE OF CONTENTS

I. Executive Summary

This report fulfills OMB's requirement under the Government Information Security Reform Act (Security Act) to submit an annual report to the Congress summarizing the results of security evaluations conducted by agencies and reported to OMB. The Security Act requires agency Chief Information Officers (CIOs) to work with agency program officials in conducting annual security reviews of all agency programs and systems. It also directs Inspectors General (IGs) to perform annual independent evaluations of an agency's security program and a subset of agency systems. OMB issued guidance in January 2001 that extended reporting responsibilities to OMB to include the results from reviews conducted by CIOs and program officials. OMB guidance in June 2001 provided specific instructions to Federal agencies and IGs on reporting the results of their reviews and independent evaluations to OMB in a detailed executive summary. This report is based largely on the agency reports to OMB, and includes findings from CIOs, program officials, IGs, and OMB. The information and findings in this report are based on work performed during FY 2001.

The body of this report discusses the steps taken by OMB and Federal agencies to implement the Security Act as well as additional efforts OMB and the agencies have taken to improve Federal information technology (IT) security. This report also lists six common government-wide security weaknesses OMB identified through review of agency Security Act reports. To appropriately address these weaknesses, Federal agencies need to: 1) greatly increase the degree of senior management attention to security; 2) establish measures of performance to ensure senior agency management can evaluate the performance of officials with security responsibilities; 3) improve security education and awareness; 4) fully integrate security into the capital planning and investment control process; 5) ensure that contractor services are adequately secure; and 6) improve their ability to detect, report, and share information on vulnerabilities.

Since the completion of their reviews, agencies have developed and begun implementing corrective action plans to resolve the security weaknesses found in the course of their reviews. These plans are required by OMB guidance issued in October 2001. This report makes general reference to these plans and their importance for resolving long-standing and new security weaknesses, but the agency specific summaries found in Appendix C, and overall findings based on the summaries in this report are not based on these correction plans. Successful implementation of corrective action plans that appropriately address all weaknesses will bring agencies a long way toward positive overall security performance, progress that will be documented in next year's report to the Congress.

To ensure that security is addressed throughout the budget process, OMB directed agencies to: 1) report security costs for their IT investments; 2) document in their business cases that adequate security controls have been incorporated into the life cycle planning of each IT investment; 3) reflect the agency's security priorities as reported in their corrective action plans; and 4) tie their corrective action plans for an IT investment directly to the business case for that investment. Additionally, OMB will require large

agencies to undergo a Project Matrix review to ensure a common methodology to identify their critical assets and interdependencies.

For FY 2002, Federal agencies reported planned government-wide spending of about $2.7 billion from a total IT investment of about $48 billion with additional spending on security from the emergency supplemental last fall. OMB estimates FY 2003 funding for IT security investments of $4.2 billion from a total IT investment request of approximately $52 billion. This figure does not include training for non-IT personnel and new Office of Homeland Security government-wide initiatives.

To intensify oversight, OMB will: 1) consult periodically with agencies to discuss progress on their corrective action plans; 2) integrate security as an element contributing to the President's Management Agenda Scorecard; 3) encourage agency IGs to monitor improvements; and 4) assist agencies in developing management-level performance measures for security.

Specific information on individual agencies can be found in two appendices to this report. Appendix A is a listing of relevant documents referenced in this report along with websites where they may be found. Appendix B provides brief summary remarks for small and independent agencies that submitted a report. Appendix C contains summaries for the 24 Chief Financial Officers (CFO) Act agencies.

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

II. Administration Security Initiatives

A. Executive Orders

The President has given a high priority to the security of government information systems and the protection of our nation's critical information assets. The President is concerned about the growing risks that our nation faces from cyber threats and the risks to our cyber assets that physical attacks can bring.

American society increasingly relies on the Federal government for essential information and services. At the same time, the Administration knows that interconnected computer systems are necessary for the provision of essential information and services. Government and industry face increasing security threats for essential services and must work in close partnership to address those risks. Indeed, this risk is also shared globally. To adequately protect the information and technology that the Federal government depends upon, agencies must resolve current security weaknesses and protect against future vulnerabilities and threats.

On October 8, 2001, the President signed Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council." This Executive Order provides for the implementation of a comprehensive national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats and attacks within the United States. Governor Tom Ridge serves as the Director for Homeland Security. Additional information on the Administration's homeland security agenda can be found in the President's FY 2003 Budget request to the Congress.

Subsequently, the President issued Executive Order 13231,"Critical Infrastructure Protection in the Information Age." This Executive Order establishes the Critical Infrastructure Protection Board and creates a Chair who serves as the Special Advisor to the President for Cyberspace Security. This Board will promote greater coordination and consistency among the Federal agencies. The Board will oversee work to ensure that: Federal policies and processes are appropriate so that critical commercial and government IT assets are adequately secure; emergency preparedness communications are operating adequately; and government and industry work closely together to address increasing interconnections and shared risk. Richard Clarke serves as Chair of the Board and Special Advisor to the President for Cyberspace Security, and reports both to Governor Ridge on issues that affect homeland security and to National Security Advisor Condolezza Rice on issues that affect national security.

The President has made OMB a member of both the Homeland Security Council and the Critical Infrastructure Protection Board. OMB's presence in both organizations reflects OMB's statutory role regarding the security of Federal information systems. OMB is responsible for focusing resources so that programs can operate more effectively and are appropriately funded. OMB chairs the Board's standing committee on Executive Branch information systems security.

Among the issues that the Office of Homeland Security and the Critical Infrastructure Protection Board will focus on is the relationship between the Federal government's programs for security, critical infrastructure protection, and continuity of government operations. In most respects these are related and complementary programs and effective implementation of one program helps promote effective implementation of the other two. At the same time, OMB wants to remove any unnecessary duplication of effort and find any wasteful expenditure of scarce resources so that collectively these programs can operate more effectively and be funded adequately.

B. Additional OMB Actions

OMB will continue to engage the agencies in a variety of ways to address the problems that have been identified, continuing to emphasize both the responsibilities and performance of agency employees in addition to accountability for exercising those responsibilities and consequences for poor performance. OMB has made it a policy to stop funding projects that do not adequately address security requirements and neglect to document how security planning and funding is integrated into the project's life cycle.

To ensure that security is addressed throughout the budget process OMB established the following four criteria:

-- Agencies must report security costs for each major and significant IT investment.

-- Agencies must document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment.

-- Agency security reports and corrective action plans are presumed to reflect the agency's security priorities and thus will be a central tool for OMB in prioritizing funding for systems.

-- Agencies must tie their corrective action plans for a system directly to the business case for that IT investment.

Additionally, OMB will take the following four steps to intensify security oversight responsibilities. The first step is integration of security as an element under the President's Management Agenda Scorecard. Secondly, OMB will consult periodically with agencies to discuss progress on their corrective action plans. Third, OMB will encourage agency IGs to monitor agency improvements. Fourth, OMB will assist agencies in developing management-level performance measures for security.

In discharging OMB responsibilities under the Security Act, OMB has communicated with the appropriate agency heads to impress upon them that true improvements in security performance comes not due to external oversight from OMB, IGs, the General Accounting Office (GAO), or Congressional committees, but from within – holding

agency employees, including CIOs and program officials, accountable for fulfilling their responsibilities. Security is the responsibility of every employee in the agency. There must be consequences for inadequate performance. This communication also underscored the essential companion to accountability -- the need for clear and unambiguous authority to exercise responsibilities.

Security Corrective Action Plans

To ensure that the reporting process does not devolve into an annual bureaucratic paper drill, OMB has required that agencies produce for their own use and report to OMB their corrective plans of action and milestones. Corrective action plans must be prepared for each weakness found by an IG evaluation, a program review, or any other review conducted throughout the year, including a GAO audit. These plans, which were submitted to OMB last fall, are important to OMB's oversight work and also to the agencies and IGs. They bring a discipline to the process, make tracking progress much easier for all involved, and should contribute to better annual reporting. OMB will provide quarterly assessments to the President's Management Council on whether corrective actions are on track. OMB judgements on the quality of corrective plans are not reflected in this report. These plans will be discussed with each agency and agency performance in implementing these plans will be reflected in next year's report.

OMB is also requiring that each of the agency program reviews, which should also include individual system reviews and plans of action be tied to the budget process through the corresponding business cases submitted with the agencies' budget. In this way, funding required to correct the weaknesses identified in the plan of action are accounted for in the agency's funding for an asset. OMB guidance is clear that unless security is incorporated into and funded as part of each investment it will not be funded.

These plans are a critical next step to assist agencies with identifying, assessing, prioritizing, allocating resources, and monitoring the progress of corrective actions and will serve as a valuable management and oversight tool for agency officials, IGs, and OMB.

Project Matrix and Enterprise Architecture

The development of a government-wide enterprise architecture is a central part of the Administration's electronic government efforts. Establishment of an architecture for the Federal government will greatly facilitate information sharing based on the lines of business of each agency. Additionally, this architecture will identify redundant capabilities and provide ample opportunities to increase efficiencies while reducing costs, and duplicative programs. Accordingly, OMB will also be able to better prioritize and fund the Federal government's security needs.

To more clearly identify and prioritize the security needs for government assets, OMB will direct all large agencies to undertake a Project Matrix review. Project Matrix was developed by the Critical Infrastructure Assurance Office 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. This is largely a vertical view of agency functions. To ensure that all critical government processes and assets have been identified, once reviews have been completed at each large agency, OMB will identify cross-government activities and lines of business for Matrix reviews. In this way OMB will have identified both vertically and horizontally the critical operations and assets of the Federal government's critical enterprise architecture and its relationship beyond government.

Electronic Government

OMB's work on expanding electronic government under the President's Management Agenda identifies security as a key issue. In fact all of the electronic government initiatives must address security. In addition to a risk management plan, Federal agencies must demonstrate for each initiative that security needs for the initiative have been assessed, appropriate security controls identified, and that the agency has a process to maintain effective security for the project over its life cycle. Underlying these initiatives is E-authentication. The goals of this initiative are to ensure the integrity of transactions and that parties to a transaction are authorized to participate in a secure manner.

III. The Government Information Security Reform Act

The Government Information Security Reform Act of 2000 (Security Act) amends the Paperwork Reduction Act of 1995 (PRA) by adding a new subchapter on Information Security. The Security Act reinforces and builds upon the Computer Security Act of 1987 and the Information Technology Reform Act of 1996 (Clinger-Cohen). Like the PRA and Clinger-Cohen, the Security Act binds agency security programs and practices to their overall program and IT management and capital planning as well as their budget processes.

The Security Act divides security programs into three basic components -- management, implementation, and evaluation.

-- For management, it recognizes that while security has a technical component, it is at its core, an essential management function.

-- For implementation, it essentially codifies OMB's security policies and recognizes that program officials (not security officers or CIOs) are primarily responsible for ensuring that security is integrated and funded within their programs and tied to the program goals. The Security Act does not introduce new technical or procedural security requirements that result in greatly increased funding needs.

The Security Act highlights the reality that when security funding and implementation are separated from operational programs, program

officials and users begin to ignore it. Separation sends the incorrect signal that it is not a program responsibility.

CIOs also have a significant role. They must take an agency-wide strategic view of implementation and ensure that the security of each program is appropriately consistent with and integrated into the agency's overall program and enterprise architecture. Security officials are also essential, but they cannot do it all.

-- For evaluation, the Security Act requires program officials and CIOs to conduct annual security reviews of all programs and systems. IGs are to perform independent evaluations of an agency's security program and an appropriate subset of agency's systems and report their findings to OMB.

A. OMB Security Act Guidance

Implementation Guidance

OMB first issued guidance to agencies on implementation of the Security Act in January 2001. This guidance focused on unclassified Federal systems and largely addressed those areas of the Security Act that introduced new or modified requirements. Its purpose was to inform agencies of their responsibilities under the new Security Act, emphasizing the evaluation and reporting requirements, and alerting agencies to future guidance on specific reporting instructions. Additionally, it emphasized the security responsibilities of agency officials, IGs, specific agencies, and OMB.

Reporting Instructions

Reporting guidance was issued in June 2001. Agencies were directed to report in an executive summary to OMB, the measures of performance used to ensure agency officials are fulfilling their security responsibilities and description of the actual level of performance of the agency in implementing their security requirements. Each topic in the reporting instructions related to a specific agency responsibility outlined in the Security Act or OMB guidance to agencies on preparing their annual budget submissions.

The Security Act's reporting requirement is relatively narrow, i.e., each agency must report to OMB the results of their IG's annual independent evaluations and OMB is to prepare a summary report to Congress.

Because security is a high priority for the Administration, OMB expanded the Security Act's reporting requirement requesting agencies to provide copies of other products they were required to prepare. In addition to reporting the IG's independent evaluations, agencies must also report the results of reviews performed by program officials and CIOs. Agencies also were asked to furnish sufficient supporting documentation to support executive level analysis of their findings.

OMB reporting guidance directed agencies and IGs to answer questions in 13 topic areas which, for the most part, address or are closely related to the major features of the Security Act and OMB policy. These areas were included to provide both background information, an understanding of how the agency conducted their reviews, and information on the agency's security program performance.

B. Management Performance

For the most part, this report focuses on management issues, not those of technical or operational implementation. OMB has found many examples of successes and promising technical and operational practices throughout government, such as the Department of Defense's (DOD) efforts known as the Information Assurance Vulnerability Alert that conducts regular vulnerability scanning and remediation for all of the agency's systems. But such tools are only as effective as the management support to use them effectively and dedicate the resources necessary to address risk.

To assist agencies in securing their IT through improved management, the National Institute of Standards and Technology (NIST) has established the Computer Security Expert Assist Team. This team performs a review of an agency's computer security program from a management, not technical, perspective.

One time risk assessments do not provide the level of security or protection needed. Relying on infrequent system penetration tests and scans to reveal vulnerabilities does little more than improve security for a moment in time. Certainly using such tools is essential, but they are not panaceas and their limitations must be understood. Because the pace at which technological threats (hackers, viruses, and worms) and vulnerabilities arise, testing and scanning must be performed nearly continuously commensurate with the risk and magnitude of harm. Clearly this is a resource intensive undertaking and underscores the imperative that program managers must ensure that such efforts are built into and funded over the life cycle of system operations. Simply tacking them on without sustained funding as part of those systems is not effective.

OMB requires that security be built into the funding of all IT investments. However, OMB also understands that some security needs cut across an agency and require separate funding for those needs. For example, the Department of Health and Human Services (HHS) has been appropriated over $20M for their "Information Technology Security and Innovation Fund." This fund will for the first time permit HHS to implement enterprise-wide security projects to address common security needs across all of HHS's components thus improving security performance throughout the Department.

IV. OMB's Government-wide Findings and Agency Security Reports

While there are examples of good security in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security. These findings are not new. OMB, GAO, IGs, and the

agencies themselves have recognized pervasive security problems for many years. Yet, prior to the Security Act reviews, In the past many security improvements had simply been in reaction to specific findings by inspectors or auditors. Only spotty efforts had been made to be continuously proactive. It is important that this reactive culture change within each agency. While OMB and others can help the agencies identify, correct, and prevent security problems, we cannot do the work for them.

A. Six Common Security Weaknesses

OMB's review of over 50 agency reports identified six government-wide security problems. Additional information is provided detailing steps OMB is taking with agencies to address these common security weaknesses.

1. Senior management attention. Overall, senior leaders have not consistently established and maintained control over the security of the operations and assets for which they are responsible. Over the past six years, GAO has recognized this problem at every agency and correction calls for more than an occasional high-level memorandum. IT security is far more than a technical issue for which IT professionals, CIOs, and security experts are responsible. It is essential to mission success. As the Security Act recognizes, security is a management function which must be embraced by each Federal agency and agency head.

   While this is a common problem, OMB commends the Department of Agriculture in particular for a clear commitment of senior management to address and resolve security weaknesses through sustained attention. This includes development and implementation of performance measures to promote accountability and allocation of appropriate resources to support remediation efforts.

   Ongoing Activity to Address this Issue: OMB is working through the President's Management Council and the Critical Infrastructure Protection Board to promote sustained attention to security as part of OMB's work on the President's Management Agenda and the integration of security into the Scorecard. OMB has also included security instructions in budget passback guidance and has sent security letters to each agency highlighting this problem and describing specific actions OMB is taking to assist the agency.

2. Measuring performance. One effective way for senior agency management to convey their interest in security and other management issues is to ensure that they evaluate the performance of officials charged with implementing specific requirements of the Security Act. To evaluate agency actions, OMB requested data to measure job and program performance, i.e., how senior leaders evaluate whether responsible officials at all levels are doing their job. Virtually every agency response regarding performance implies that there has been inadequate accountability for job and program performance related to IT security.

The Chief Information Officers Council and NIST developed a security assessment framework to assist agencies with a very high level review of their security status. Building from this framework, NIST issued a more detailed security questionnaire that most agencies used to conduct their program and system reviews.

Every Federal agency needs to devote immediate and increased attention to establish measures of performance. While no agency has fully developed and implemented appropriate measures, a handful of agencies described initial efforts in their reports. Reports from the Department of Veterans Affairs, the General Services Administration, and the Social Security Administration demonstrated the initial work they had begun to define performance measures for their CIO and program officials.

Ongoing Activity to Address this Issue: OMB is working with the agencies and others to develop workable measures of job and program performance to hold Federal employees accountable for their security responsibilities. In addition, IT security improvements will be evaluated quarterly as part of the President's Management Agenda Scorecard.

3. Security education and awareness. Despite being specifically required by law since the Computer Security Act of 1987, Federal agencies continue to perform poorly in this important area. Some agencies and large bureaus reported virtually no security training. This is the opposing bookend to senior management attention -- ensuring that general users, IT professionals, and security professionals have the adequate knowledge to do their jobs effectively and securely. Government employees must understand their responsibilities before being held accountable for them.

   DOD operates the most comprehensive security training program of any Federal agency. DOD mandates annual IT security awareness training for all military and civilian employees, provides specialized training for employees with significant IT security responsibilities, and certifies all users prior to permitting access to IT networks. The Department uses a number of different methods to conduct training, including video, computer, and web-based training.

   Ongoing Activity to Address this Issue: OMB and Federal agencies are now working through the new Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. Additionally, the CIO Council's Best Practices Committee is working with NIST through NIST's Federal Agency Security Practices website to identify and disseminate best practices involving security training. Finally, one of the Administration's electronic government initiatives is to establish and deliver electronic-training. This initiative will provide e-training on a number of mandatory topics, including security, for use by all Federal agencies, along with State and local governments.

4. Funding and integrating security into capital planning and investment control. Another important way to ensure sustained senior management attention is to tie security to the budget process. To make security successful, agency officials must

ensure that it is built into and funded within each system and program through effective capital planning and investment control. As OMB has done for the past two years in budget guidance, Federal agencies were instructed to report on security funding to underscore this fundamental point.

Two agencies in particular stand out in this area. Both the Department of Housing and Urban Development and the Department of Labor have taken steps to fully integrate security into their capital planning processes. This effort was demonstrated in the agencies' Security Act reports and their IT budget materials. OMB commends them for their work. Additionally, the Department of Education and the Federal Emergency Management Agency have taken appropriate steps in this direction.

Ongoing Activity to Address this Issue: OMB is aggressively applying this approach 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. The IT investment justification and documentation process is key to sound program and financial management. Security must not be viewed differently. This process demonstrates explicitly how much agencies are spending on security and associates that spending with a given level of performance. Thereafter, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved performance. This is the security component of the business case.

5. Ensuring that contractor services are adequately secure. Given that most Federal IT projects are developed and many operated by contractors, IT contracts need to include adequate security requirements. Although laws and policy have required contractual security requirements for many years, the agency reports reveal ongoing weaknesses. Many agencies have reported no security controls in contracts or no verification that contractors fulfill any requirements that may be in place.

   While nearly every IG reported room for improvement in this area of security, the IGs' reports from both DOD and the Office of Personnel Management recognize the significant work both agencies have done in ensuring contractor provided services are adequately secure and meet current security requirements.

   Ongoing Activity to Address this Issue: Under the guidance of the OMB-led security committee established by E.O. 13231, an issue group will develop recommendations, to include addressing how security is handled in contracts themselves. OMB will work with the CIO Council and the Procurement Executives Council to establish a training program that ensures appropriate contractor training in security.

6. Detecting, reporting, and sharing information on vulnerabilities. Far too many agencies have virtually no meaningful system to test or monitor system activity and therefore are unable to detect intrusions, suspected intrusions, or virus infections. This places individual agency systems and operations at great risk since response depends on detection. Perhaps most significant, not detecting and reporting IT security problems could cause cascading harm. Our vastly inter-networked

environment also means an environment of shared risk with the best security being only as strong as the weakest security.

Early warning for the entire Federal community starts first with detection by individual agencies, not incident response centers at the FBI, GSA, DOD, or elsewhere. The latter can only know what is reported to them, reporting can only come from detection, and guidance for corrective action depends upon both. This need is thus not a technical one, but a management one. Program officials must understand and execute their individual responsibilities. Additionally, it is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center and appropriate law enforcement authorities such as the FBI's National Infrastructure Protection Center as required by the Security Act.

Both the State Department and the Agency for International Development were recognized by their IGs for their work in establishing incident response capabilities and ensuring active virus detection programs for their systems. Both agencies noted that independent penetration tests failed to penetrate their networks firewalls.

Ongoing Activity to Address this Issue: GSA's Federal Computer Incident Response Center reports on a quarterly basis to OMB on the Federal government's status on IT security incidents. Additionally, under OMB and Critical Infrastructure Protection Board guidance, GSA is exploring methods to disseminate patches to all agencies more effectively.

Since the submission of their reports Federal agencies have been working to develop and implement corrective action plans that address the six common weaknesses listed above and others found during their reviews. For example, last year the Department of Justice developed a comprehensive database that the agency is using to track and remedy security weaknesses system by system. This database is a single repository of findings and corrective actions identified through component certification and accreditation activities, IG audits, Department penetration testing, and other reviews.

B. Challenges to Securing IT

Some aspects of securing information systems are currently beyond any organization's (in government or industry) direct control. A primary issue is that basic operating systems for desktop computers and other commercial software is produced, delivered, and implemented with an alarming number of security weaknesses. While some of these weaknesses are known and can be corrected during implementation and testing, others are unknowable until very sophisticated (and time consuming) tests are performed, or worse, until a hacker exploits them.

Two recent examples underscore this point. First is the case of the Code Red worm. It propagated and infected systems at such a rate that it moved faster than anyone's ability to download and install the necessary corrective patches. Second is the serious security

weakness found in the latest operating system of a major software company. Despite years of development and testing, the weakness was not discovered until millions of copies had been sold to consumers. While a corrective patch was quickly available, history tells us that operating systems of this complexity invariably have many more serious security weaknesses that are yet to be discovered.

As long as commercial software contains security weaknesses, agencies must be prepared to manage an unacceptable level of risk. This again underscores the point that agencies must understand the risk to their operations and assets and program officials must assure that continuous monitoring and testing is built into and funded in their IT investments.

A number of efforts are underway to address security weaknesses in industry software development. Chief among them are national policy-level activities of the Critical Infrastructure Protection Board. At the technical product-level, the National Information Assurance Partnership, operated jointly by NIST and the National Security Agency, is certifying private sector laboratories to which product vendors may submit their software for analysis and certification. But this certification process is a lengthy one and often cannot accommodate the "time-to-market" imperative that the technology industry faces.

C. Frequent Security Questions

Since enactment of the Security Act a number of questions have been frequently asked. Because of their relevance to this report they are addressed below.

1. Is OMB going to assign grades to the agencies?
   No. OMB has not assigned grades to agencies. However, for the President's Management Agenda Scorecard OMB has made public the red, yellow, or green scores assigned to each agency, and security will be incorporated into the Scorecard. The Security Act gives OMB the authority to approve agency security programs and through private communications with the agencies, OMB did conditionally approve some programs and did not approve others. The decision to conditionally approve or not approve an agency security program was based on OMB's review of the agency's FY01 Security Act report, the manner in which security had been integrated in the agency's capital planning process, and the criteria laid out in OMB policy and the Security Act. This information was reported to OMB in agency Security Act reports that covered a specific reporting period (from November 2000 to September 2001) and budget materials. It did not include corrective actions taken by an agency since the submission of their report to OMB in September. Therefore agency security plans of action and milestones required by OMB guidance were not a factor in the decision to conditionally approve or not approve an agency security program, since under the statute OMB's decision is based on the agency's existing program. OMB anticipates reporting on the progress agencies have made in next year's report.

2. How much does the Federal government spend on security?
   For FY 2002, agencies reported planned government-wide spending of about $2.7 billion from a total IT investment of about $48 billion with additional spending on

security from the emergency supplemental last fall. Table 1, *FY 2002 Agency IT and IT Security Spending*, reports planned IT security and IT spending for the 24 CFO Act agencies. OMB estimates FY 2003 funding for IT security of $4.2 billion from a total IT investment request of approximately $52 billion.

3. Is the Federal government spending enough on IT security?
Nearly sixty percent of the Federal agencies reported spending between 2.1 and 5.6% of their total IT investment on security. Five agencies reported spending between 7.3 and 17% and five reported between 1.0 and 2.0%. OMB assessed the agencies' security performance against the amount they spent on IT security and did not find that increased security spending equals increased security performance.

Therefore, at this point, there is no evidence that poor security is a result of lack of money. Rather improvements in security performance will come from agencies giving significant attention to the six security weaknesses described above.

Over the past several years there have been many calls for a security fund commensurate with what Congress approved for Y2K remediation. Y2K spending totaled some $8 billion over four years. Security spending is on the order of $10-12 billion every four years. As the reported figures indicate, the Federal government spending on security exceeds Y2K remediation costs.

There are many security functions that would greatly benefit and be more cost effective if employed in a cross-government enterprise-wide approach, not piece meal funding within individual agencies. A consistent and comprehensive training program for Federal employees is one example. Other examples include:

-- The Administration's electronic government initiative on E-authentication which seeks to ensure that parties to a transaction are authorized to participate and ensure the integrity of the transaction; and

-- Development of a government-wide enterprise architecture for the Federal government to facilitate information sharing based on the lines of business of each agency. Additionally, this architecture will identify redundant capabilities and provide ample opportunities to increase efficiencies while reducing costs. Accordingly, OMB will also be able to better prioritize and fund the Federal government's security needs.

Table 1. FY 2002 Agency IT and IT Security Spending
(in millions)

Agency	IT Security Spending	IT Spending	Security as a % of IT Spending
Agency for International Development	4.2	76	5.5
Agriculture	15	1,492	1
Commerce	25	947	2.6
Defense	1,770	23,643	7.5
Education	11.5	575	2
Energy	109	1,159	9.4
Environmental Protection Agency	9.2	361	2.5
Federal Emergency Management Agency	2.9	166	1.8
General Services Administration	14.8	455	3.3
Health and Human Services	62	4,237	1.5
Housing and Urban Development	9.6	376	2.6
Interior	17.2	628	2.7
Justice	79.3	2,093	3.8
Labor	67	393	17
National Aeronautics and Space Administration	105	2,558	4.1
National Science Foundation	1.56	30	5.2
Nuclear Regulatory Commission	1.4	64	2.2
Office of Personnel Management	4.3	92	4.7
Small Business Administration	2.85	39	7.3
Social Security Administration	38.5	742	5.2
State	81	897	9
Transportation	50.9	2,514	2
Treasury	174.7	3,098	5.6
Veterans Affairs	54.7	1,181	4.6
TOTAL	**2,712**	**47,815**	

D. Quality of Agency Reports

Given that this is the first year for reporting, the overall efforts demonstrated by the agencies is noteworthy. Many agencies submitted reports that were complete and provided sufficient detail to support their findings. Where incompleteness was found, OMB and the agencies resolved it through subsequent consultation. For the most part it is clear that agencies and IGs took great pains to conduct the program and system reviews needed to prepare complete security reports.

Unfortunately, some agencies failed to review each of their systems and programs as required by the Security Act. Some attribute this failure to the lateness of specific guidance on how to conduct such a review. However, program and system security planning, certification, control testing, and periodic review have been explicitly required by law and policy since the Computer Security Act of 1987. Next year's reports should reflect a review of all systems and programs. Indeed, such reviews should already be underway. To facilitate these reviews, NIST has been automating its system and program assessment tool, but clearly this tool will not be self-executing. The agencies must employ careful and thoughtful analysis to ensure an adequate product.

Some of the reports from the CIOs were quite candid and revealed problems that one might expect to come only from an IG. Regrettably, at the same time, other serious problems were known and not reported at all by CIOs or IGs. Based on discussions with agency officials, OMB expects that next year's reports will not exhibit such gaps.

V. Conclusion

OMB views this report, along with agencies' Security Act reports, as a valuable baseline to record agency security performance. The reporting requirements of the Security Act have afforded agencies, IGs, GAO, OMB, and Congress the ability to capture this baseline with more detailed information than has previously been available. As mentioned earlier, OMB has taken steps to maximize this opportunity through additional guidance requiring agencies to develop and submit initial corrective action plans that address all security weaknesses found in reviews, evaluations and other audits. Federal agencies are instructed to provide OMB brief quarterly updates on their progress in implementing their plans. Agencies are now moving forward from their baselines and are working to improve the security of their information and technology through implementation of these corrective action plans.

Despite the security challenges the Federal government faces, OMB is not delaying our aggressive move towards accomplishing the President's Management Agenda, including using secure IT to make government more effective, responsive, and citizen centric. OMB will continue to rely on traditional budget and management processes to ensure that IT security needs are being addressed. Working together, the Federal government can and will accomplish its IT security goals.

VI. Additional Information

Appendix A is a listing of relevant documents referenced in this report along with websites where they may be found.

Appendix B provides brief summary remarks for small and independent agencies that submitted a report.

Finally, Appendix C of this report summarizes the security reports for all 24 CFO Act agencies. Each summary is organized by the 13 topic areas set forth in the OMB reporting guidance. Where appropriate, the source of the information is noted as being from either the agency or the IG.

Appendix A: Security Documents Referenced in OMB Summary Report

1. The Government Information Security Reform Act

   //csrc.nist.gov/policies/Subtitle-G2.pdf

2. OMB Memorandum 01-08, *"Guidance On Implementing the Government Information Security Reform Act,"* January 16, 2001

   www.whitehouse.gov/omb/memoranda/m01-08.pdf

3. OMB Memorandum 01-24, *"Reporting Instructions for the Government Information Security Reform Act,"* June 22, 2001

   www.whitehouse.gov/omb/memoranda/m01-24.pdf

4. OMB Memorandum 020-01, *"Guidance for Preparing and Submitting Security Plans of Action and Milestones,"* October 17, 2001

   www.whitehouse.gov/omb/memoranda/m02-01.html

5. OMB Circular A-130, *"Management of Federal Information Resources,"* Appendix III, *"Security of Federal Automated Information Resources"*

   www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

6. Additional technical security guidance from the National Institute of Standards and Technology's Computer Security Resource Center can be found at //csrc.nist.gov/publications/

Appendix B: Security Act Reporting by Small and Independent Agencies

The Security Act amended the Paperwork Reduction Act of 1995 (PRA) and added a new subchapter on Information Security. As a result, all agencies previously covered under the PRA are also responsible for fulfilling the requirements of the Security Act. In addition to the 24 CFO Act agencies, 35 small and independent agencies submitted reports to OMB.

OMB recognizes that many of the small and independent agencies are considerably smaller in size and have far fewer available resources than the larger 24 CFO Act agencies. Even so, it was clear that many conducted extensive reviews and OMB commends them for their work. These small and independent agencies have also submitted corrective action plans and are currently working on resolving their security weaknesses, and will be providing quarterly updates to OMB.

Generally, the small and independent agencies' reports revealed that they face the same security problems as the 24 CFO Act agencies. This includes inconsistent methods of ensuring contractor provided services are adequately secure, inadequate security training for all employees, lack of measures of performance to ensure that security responsibilities throughout the agency are being fulfilled, lack of fully implemented intrusion detection capabilities with agency-wide sharing, and inadequate integration of security into the agencies' capital planning processes. Additionally, many small and independent agencies need to immediately develop a documented agency-wide security plan (this activity should be addressed in the agency's corrective action plans.) At the same time, many of the small and independent agencies recognized these weaknesses and reported in their reports immediate steps they began to address them. OMB plans on working with the small and independent agencies through the Small Agency Council to address these issues.

The small and independent agencies that submitted reports are listed below.

Broadcasting Board of Governors
Commodity Futures Trading Commission
Consumer Product Safety Commission
Corporation for National and Community Service
Defense Nuclear Facilities Safety Board
Equal Employment Opportunity Commission
Executive Office of the President
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
National Archives and Records Administration
National Credit Union Administration
National Endowment for the Arts
National Endowment for the Humanities
National Labor Relations Board
Occupational Safety and Health Review Commission
Overseas Private Investment Corporation
Peace Corps
Pension Benefit Guaranty Corporation
Postal Rate Commission
Railroad Retirement Board
Selective Service System
Tennessee Valley Authority
U.S. Chemical Safety and Hazard Investigation Board
U.S. International Trade Commission
U.S. Merit Systems Protection Board
U.S. Office of Special Counsel
U.S. Patent and Trademark Office
U.S. Securities and Exchange Commission

Appendix C: Individual Agency Summaries for the 24 CFO Agencies

The summaries found in this appendix are organized by the thirteen topic areas Federal agencies reported to OMB per reporting instruction guidance. OMB guidance instructed Federal agencies to report on the following information:

- security spending;
- number of programs reviewed (the Security Act required program officials and CIOs review all programs and systems);
- methodology used to review;
- whether they found material weaknesses reportable under other law, e.g. the Chief Financial Officers Act of 1990 and the Federal Managers Financial Integrity Act.
- how they measure the performance of agency officials in fulfilling their security responsibilities;
- the effectiveness of training programs;
- how they detect and report vulnerabilities;
- how they integrate security and capital planning;
- how they prioritize and protect critical assets;
- how they ensure security plans are implemented;
- how they integrate all security programs; and
- how they ensure secure contractor performance.

The information in these summaries was provided to OMB from CIOs, agency program officials, and IGs and represents the results of their management reviews and independent evaluations. Where appropriate, OMB analysis on an agency's integration of security into their capital planning process has been added. Federal agencies largely demonstrate their work in this area through submission of IT budget materials.

It is important to note that the agency summaries found in this appendix do not address corrective actions Federal agencies have taken or plan to implement. These summaries are based on agency performance during FY 2001.

Agency for International Development

1. ***Security funding.***
   The Agency for International Development reports planned FY 2002 funding for IT security and critical infrastructure protection of $4.2M. This level of funding comprises 5.5% of their total planned IT portfolio of $76M.

2. ***Number of programs reviewed.***
   The Agency reviewed 8 major applications and systems that are identified as mission critical. The Security Act and OMB guidance call for a review of all programs and systems. The IG limited their evaluation to four of these systems.

3. ***Review and independent evaluation methodology.***
   The Agency reported using the Federal CIO Council IT Security Assessment Framework criteria as the methodology to review IT security for their major systems and applications. They also performed self-evaluations using checklists developed from Security Act requirements, Federal and Agency policies, and interviews with Information System Security Officers. The IG reviewed documentation, interviewed officials, and compared the Agency's IT security practices with guidance set forth in the Security Act, the GAO's Federal Information System Controls Audit Manual, OMB policies, and the Clinger-Cohen Act of 1996. The IG also contracted for penetration testing and general controls audits to provide additional support for their conclusions.

4. ***Material weaknesses.***
   The Agency has reported IT security material weaknesses for many years. The Agency and IG concur that information system security continues to be a material weakness. Furthermore, the IG found that the Agency had not implemented an effective IT security program that meets the requirements of the Computer Security Act of 1987 or OMB policies. The Agency reports that it is unable to resolve these deficiencies until FY 2003.

   The IG reports that deficiencies exist in virtually all areas of the Agency's IT security program and cites inadequate management controls as the underlying cause. This includes the need for organizational structures that clearly delegate responsibility and authority, planning policies that provide an effective program framework, and implementation of key processes. The Agency is taking steps to rectify this situation, but it will be some time before they are compliant with the Security Act and other relevant statutes. At the same time, it is important to note one significant bright spot -- IG commissioned penetration tests were unable to penetrate the Agency's network from outside the firewall.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency did not report any measures of performance used to ensure officials assessed risk, determined security levels, maintained plans and tested controls, or

examples of actual performance realized against those metrics. The report does mention how they plan to improve their security program, such as conducting risk assessments, conducting cost benefit analysis to determine security levels, developing security plans, and regularly scanning systems for vulnerabilities. The report says that "assessments are being conducted as resources permit" but doesn't say what efforts are being taken to identify such resources or what priority such efforts have been given. While the Agency's report does not indicate it as a priority, one performance measure is system certification and in this area the Agency is deficient. The report shows three of eight mission critical systems are certified (one of which needs to be updated), but three are not even scheduled for certification. Defining and tracking performance is a key feature of a viable IT security program, and the lack of specific information in this area raises concerns how the Agency can effectively ensure adequate levels of performance by program officials. The IG assessment found that while the Agency recognizes the need to develop and initiate an agency-wide information security program, such a program has not been fully implemented.

6. ***Measures of performance used by the Agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The Agency did not report any performance measures used to ensure the CIO has effectively implemented and maintained security programs and trained employees, nor did they provide examples of actual performance realized. The Agency reports that reforms are underway that assign the CIO responsibility for defining measures of performance. However, the IG found that the CIO's effectiveness is compromised because they do not report directly to the Administrator and therefore may not be able to provide the necessary leadership, oversight, and enforcement. The IG also reported that the current approach to IT security lacks a centralized function to ensure that the necessary practices are implemented.

7. ***How the agency ensures employees are sufficiently trained.***

   The Agency reports that its agency-wide cyber-security training has not been effective, but is in the process of formalizing it. Security awareness training is given to most new hires during orientation, but the IG found that annual refresher briefings were not being provided for all employees. The Agency reports spending $380,000 on training their 2,700-employee work force, which averages $140 per person, but there is no apparent effort to determine the types of specialized training required. Although the Agency has initiated some web-based instruction and self-taught tutorials, the IG concluded, "mission staff were not adequately trained to carry out their security responsibilities."

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***

   The Agency reports it has recently published draft procedures for incident handling, and has established a pilot Information Assurance Data Fusion Center that they plan to evolve into a Cyber Defense Center. An incident response team that is staffed during normal working hours complements the center's activities. Significant IT security incident information is shared with GSA's Federal Computer Incident

Response Center. Two incidents were reported during a three-month period in FY 2001. The IG noted that incident response reporting has not been fully implemented and does not provide timely reports of identified incidents.

9. ***Agency integration of security and capital planning.***
The Agency has no methodology for integrating security into its capital planning and investment control process. Moreover, they did not identify IT security costs and requirements in their FY 2002 capital asset plans in their budget submission to OMB. The Administrator recently approved the establishment of an IT Council to provide investment control for information systems and the Agency has developed a plan for capital planning. However, the IG found that the plan does not provide managers clear guidance on how to report IT security requirements or address the integration of IT security. As a result the Agency has not provided evidence that they are in a position to correct this problem.

10. ***Critical asset prioritization and protection methodologies.***
Beyond relying on the expert opinion of senior Agency leaders (e.g., Chief Financial and Information Officers), there is no methodology to identify and prioritize Agency mission critical systems. The Agency has taken steps to revise and update their continuity of operations plan and further identify and prioritize their assets, but they recognize that they need to better support their architecture and many activities remain to be identified and evaluated. The Agency did not indicate the plan to adopt any existing systematic methodology such as Project Matrix to accomplish this objective. The IG found that their methodology to identify and prioritize assets needs strengthening. They have established layers of security to protect their systems, but a number of safeguards are undefined or lack guidance for implementation.

11. ***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 reported only one quantifiable measure for how the Administrator ensures the Agency's IT security plan is practiced throughout a systems lifecycle. They reported no examples of actual performance. The measures of performance cited, e.g., "effectiveness of mandated reports, the quality of guidance and direction, and implementing industry-wide best practices," were too general and high level to permit real measurement. No data was provided for the only quantifiable metric, "reduction in the quantity of outstanding audit findings" other than "making progress." The performance measure reported by the IG was that four of eight systems had completed security plans. While the Agency did not do so, one would expect a report on performance against network penetration tests. As mentioned earlier, the IG tests were unable to penetrate the Agency's network. This performance indicates a level of technical success despite program management weaknesses.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Agency indicated that their continuity of operations plan is being revised and they are in the process of further identifying and prioritizing their critical IT assets. No mention was made of how IT security is being integrated with physical and operational security programs. Although Presidential Decision Directive-63 tasked Federal agencies to develop critical infrastructure protection plans, the Agency asserts that the Department of State has responsibility for the Agency's critical infrastructure protection planning, but provides no information that State is actually doing so. OMB is consulting with the Department of State on this point. The IG found that if the Agency effectively implemented an IT security program it would also protect its systems that are part of the nation's critical infrastructure.

13. ***Agency methods to ensure contractor services are secure.***
    The IG found that "[the Agency] does not have a documented methodology to evaluate if contractor-provided services are meeting security requirements." The IG also noted that status reports for mission critical systems operated for the Agency by contractors were requested by the Agency but had not been received as of the report date. Progress on this area should be included in the Agency's plan of action and milestones.

Department of Agriculture

1. ***Security funding.***
    The Department of Agriculture reports planned FY 2002 funding for IT security and critical infrastructure protection of $15M. This level of funding comprises 1.0% of their total planned IT portfolio of $1.5B.

2. ***Number of programs reviewed.***
    The Department focused their reviews on security program functions such as administration, communication, risk analysis, configuration management, etc., across all of the Department's component agencies. The initial report did not identify the number of programs reviewed, but the Department has subsequently advised that all 31 of its security programs were reviewed. The Security Act and OMB reporting guidance required a review of all programs and systems.

3. ***Review and independent evaluation methodology.***
    The Department states that they recognize the need for precise security measures of performance, but has not published them in policy or guidance. They report that they have promulgated internal and Department of Justice standards throughout the Department and use self-assessment tools that are based on OMB policy and NIST guidance. However, they do not indicate how these tools fit into a Department-wide methodology used to evaluate IT security programs. For next year's reviews, the Department should ensure that its assessment methodology at a minimum includes the complete NIST self-assessment guide and GAO's Federal Information System

Controls Audit Manual. OMB has also reminded the Department that direct application of "standards" developed by other agencies requires careful study and OMB policies and NIST guidance are determinative.

4. ***Material weaknesses.***
   Despite a history of reporting of weaknesses in their security program and security for individual systems, the Department still has serious weaknesses in virtually every aspect of their IT security program. The IG reports weaknesses in physical security, computer access controls, network and system susceptibility to intrusion, insufficient planning, no certification standards, inadequate contingency plans, and most importantly, "for the most part senior managers are not involved…"

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   The Department is still in the early stages of developing a security risk management program and assessment tools. The IG noted that only two of eleven bureaus had even assessed risks or initiated a plan for their mitigation. The Department's report provided essentially no information on the measures of performance used by officials to ensure they have assessed risk, determined security levels, maintained plans or tested controls; and there is no indication that the Department is in compliance with these requirements of the Security Act. They report they are in the process of engaging contractors and other industry experts to assist with these activities, but they do not seem to be taking advantage of the plans and assessment tools previously developed and in use by other Federal departments and agencies, e.g. NIST's self-assessment guide.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Department does not report any specific measures of performance used to ensure that the CIO has adequately maintained a Department-wide security program, effectively implemented an IT security program, or trained employees with significant IT security responsibilities. The Department indicates that they have begun to make progress and give several examples such as drafting policies, chartering advisory councils to facilitate program officials' dialogue, provided structured training courses, and working to design a security architecture. These actions are certainly an important first step, but fail to address the requirements of the Security Act. The Department's report indicates an immature IT security program and a lack of Department leadership in this area.

7. ***How the agency ensures employees are sufficiently trained.***
   The Department reports that IT security training needs improvement and is not uniform across the Department. Their report indicates that some bureaus have made training a priority, but give no indication of how the Department ensures that employees are sufficiently trained as required by the Security Act. They further state "Unless additional funding is received expressly for this purpose it is doubtful that

security awareness will improve substantially." The Department is encouraged to identify sufficient resources within their programs to address this need and ensure that future program investments incorporate and fund security throughout their lifecycle consistent with the Security Act and OMB policy.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   The Department reports the implementation of an effective incident response capability at the Department level, but does not provide any information on its actual performance. The IG reported that just three of the four bureaus they evaluated have incident response procedures in place. Despite recent progress in this area, the Department recognizes that additional work is necessary to develop an effective intrusion detection program in all bureaus and to ensure that the Department meets the requirements of the Security Act.

9. ***Department integration of security and capital planning.***
   The Department reports including more rigorous requirements for identifying security controls, costs and schedules in their capital planning process. They also report they have developed guidance for the FY 2003 budget process that includes comprehensive planning for cyber security. However, they do not fully explain how they ensure IT security is integrated into their capital planning and investment process, nor do they report whether security requirements and costs were reported on all FY 2002 capital investment plan.

10. ***Critical asset prioritization and protection methodologies.***
    As part of the Year 2000 program assessment, the bureaus of the Department of Agriculture identified 362 mission critical systems of which the CIO plans to focus attention on 52 that have been identified as top priority. The report did not describe the methodology used by the Department to identify, prioritize, and protect critical assets. Without a Department-wide methodology for identifying their critical assets and their mutual dependencies, the Department will not be able to determine adequate levels of protection for its IT systems.

11. ***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 report contains no information about the measures of performance used to ensure the Department's IT security plans are practiced throughout the lifecycle of each IT system. In the absence of this information, it appears that the Department has failed to comply with these requirements of the Security Act. The Department reports that security plans "in a large part" meet federal requirements and new guidance requires annual submission and review of the plans. This falls short of measuring effective security program management.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department reports that they have prepared a Critical Infrastructure Assurance Plan in accordance with Presidential Decision Directive 63, "Critical Infrastructure

Protection" and is aggressively implementing tools for risk assessments. They also report that their bureaus are performing self-assessments for the first time. Although these are important steps in the development of an IT security program, the report fails to provide the information requested by OMB. The Department does not give any clear indication of how they have integrated IT security with their critical infrastructure protection responsibilities, or with their physical and operational security.

13. ***Department methods to ensure contractor services are secure.***
The majority of bureau security managers within the Department report that they do not review contractor services to ensure security controls are adequate. The IG found that of the four bureaus they reviewed, most do not ensure that contractors perform proper security clearance or background checks or that contractor employees are adequately trained. The Department has failed to establish effective Department-wide methods to ensure that contractor provided IT services are adequately secure as required by the Security Act.

Department of Commerce

1. ***Security funding.***
The Department reports planned FY 2002 funding for IT security and critical infrastructure protection of $25M. This level of funding comprises 2.6% of their total planned FY 2002 IT portfolio of $947M.

2. ***Number of programs reviewed.***
The Department reports that it reviewed 514 major programs and applications. The IG reviewed four program areas comprising some 55 programs and another 94 associated systems. The IG evaluation also capitalized on reviews conducted by GAO.

3. ***Review and independent evaluation methodology.***
The Department used the NIST self-assessment guide to review their information technology systems. They reviewed some 33% of their systems while the Security Act and OMB guidance call for a review of all programs and systems. The IG used GAO's Federal Information System Controls Audit Manual as a guide for reviewing systems, as well as the results from reviews conducted by other expert parties.

4. ***Material weaknesses.***
Despite a history of weaknesses in their security program and security for individual systems, the Department is in the mode of evolving and developing security plans. While planning is essential, this has been an explicit statutory requirement since the enactment of the Computer Security Act of 1987 and by now, the Department should be executing reliable established processes including implementing and testing security plans and controls and assessing security performance. The Department has

only begun to implement its restructured IT management controls in the last several months and has yet to realize the expected benefits.

Material weaknesses have been identified and are being corrected. The IG characterizes weaknesses in information security as one of the Department's top ten management challenges. Recent penetration testing "revealed pervasive computer security weaknesses that place sensitive Commerce systems at serious risk." The IG pointed out that the lack of a policy or process for reporting information security deficiencies as material weaknesses hampers the ability to identify weaknesses. Four of the bureaus (operating units) had "reportable" management control weaknesses that "constituted a material weakness in the audit of the consolidated financial statements."

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
The Department has established policies and rules directing that program officials give IT security a high priority, sufficient resources, and their personal attention. These policies will only bear fruit if the necessary focus and leadership is maintained throughout the Department. Beyond issuing memorandum to operating unit heads, the report does not say how the program officials will be motivated to ensure they have assessed risks, determined security levels, maintained plans, and tested controls; or how these policies will be enforced. It is essential that the Department address this deficiency as past IG reports show that the Department has not carried out these fundamental responsibilities.

   The Department reports that 73% of its sensitive or classified major applications and systems have security plans in place and 64% are certified. This is a significant improvement over last year, but leaves open concerns about the possible vulnerabilities for the 36% of the systems that have not been certified. It is important to note that like planning, certification prior to beginning system operations is a longstanding requirement. Also, the report is not clear, but the IG implies that the Department has not correctly identified their classified systems and thus may not have evaluated them despite their special sensitivity.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
Each bureau CIO has as part of their performance plan the responsibility for IT management and oversight of a sound IT security program. They in turn have IT security officers reporting to them that are responsible for their unit's compliance with IT security regulations. However, their authority or their means to enforce the rules and discharge their responsibilities is not explained, nor are any specifics provided on how the training of employees is ensured other than to cite examples of future plans and proposed staff augmentations.

The IG reports that the Department is restructuring IT management to give the CIO increased authority to improve their effectiveness, but "substantial improvements are needed." With regard to employee training, there still remain "pervasive weaknesses" in controls, intrusion detection, out of date software patches and physical security. Moreover, training is not conducted on a rigorous or ongoing basis. The Department reports that the IG used GAO findings that were issued in May 2001 and its own review ended in September 2001 and thus may not reflect an accurate view of today's security posture at the Department. This is of course the unfortunate nature of program reviews and reports -- they lag behind real time status. Throughout the coming year, and in next year's report, Commerce will have the ample opportunity to report on actual progress.

7. ***How the agency ensures employees are sufficiently trained.***
The Department has established annual training programs, but the resources devoted to training are not uniform across all bureaus and the reporting was incomplete. The submitted representative sample of staff and training budgets indicate a total work force in excess of 27,560, with at least 400 categorized as systems administrator/specialist. For the bureaus that reported, fiscal year 2001 security training costs were approximately $250 for each key system administrator, and averaged less than $10 per employee for security awareness training. (In some bureaus the average was between $2 to $6 per employee.) Despite specific training requirements in the Computer Security Act of 1987, Commerce as a Department does not devote adequate resources to training. This observation is supported by the IG findings that many operating units exhibited weaknesses in IT security awareness and were not able to identify who had received training or the cost to provide it. However, the Department has provided to OMB more detailed information indicating that they have already begun increasing training resources and several operating units are now training over 70% of their employees. OMB expects the Department to use their plan of action and milestones to track progress in this area.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
Reporting practices across the Department are mixed. Some bureaus have robust tracking and reporting systems that indicate the frequency of incidents while other bureaus' reporting systems are deficient and appear to report very few incidents. The IG stated that only 4 of the 15 bureaus have formal incident response capabilities and that most bureaus have weak or nonexistent intrusion detection and auditing. Deficient detection and auditing invariably results in a low number of reported incidents and places operations and assets at risk.

The Department states that it is aware of these shortcomings and strengthened their detection and reporting by putting in place a memorandum of agreement between its CIO, IG, and their Office of Security. The Department has provided to OMB additional information indicating that all bureaus are now fully supported by a formal incident response team. The Department should use their plan of action and milestones to track progress in this area.

9. ***Department integration of security and capital planning.***
Capital planning is reported as being well-integrated at the most senior levels. A review board chaired by the CIO serves as an advisor to the Secretary for critical IT investments. IT security and risk management are said to be an integral part of the Department's investment planning process. The IG reports that capital asset plans for FY 2003 address security issues better than the FY 2002 plans, several of which did not cover security, and most did not include security costs. Many of the FY 2003 plans do a better job of identifying security requirements and explaining cost estimates. While perhaps progress has been made since FY 2002, OMB's midsummer capital planning review revealed significant deficiencies in this area and our early review of the FY 2003 budget submission shows only marginal improvement. Integration of security into a sound capital planning process is a linchpin for good security across an enterprise.

10. ***Critical asset prioritization and protection methodologies.***
The Department's Critical Infrastructure Assurance Office has developed for government-wide use a critical asset and enterprise architecture identification methodology known as Project Matrix. This project also identifies links and interdependencies between key systems and applications within and outside an individual agency. The Department has begun a Project Matrix review, but has not completed the inventory and prioritization of critical assets. The IG found that the processes used to gather data is weak and the asset inventory is questionable. OMB has found Project Matrix to be a valuable tool and have instructed all large agencies to schedule such a review; however, the value of the methodology is only as good as the data upon which it is based. The Department's three largest bureaus have expressed concerns that the inventories do not reflect the priorities of their assets, but neither they nor the Department report any effort to remedy the shortcomings. The Department has subsequently reported that a refined asset identification process "was to begin in September 2001." OMB looks forward to seeing the results of this refinement.

11. ***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 Commerce Secretary has issued a memorandum directing the bureau heads to work closely with their respective CIO, and allocate sufficient resources, and devote sufficient personal time to ensure full compliance with IT security directives. The CIO's authority stems primarily through his ability to influence the Secretary to require the bureaus to take the actions necessary to ensure IT security. Although all IT workers have IT security as an element of their performance plan, it is not clear whether Department officials have similar incentives. This is where attention to security is essential.

Despite a history of weaknesses in their security program and security for individual systems, the Department appears to still be in the mode of developing security plans. While planning is essential, this has been an explicit statutory requirement since the enactment of the Computer Security Act of 1987 and by now, the Department should

be executing reliable established processes including implementing and testing security plans and controls and assessing security performance. The Department has only begun to implement its restructured IT management controls in the last several months and has yet to realize the expected benefits. The IG believes that Department policies need to be updated and oversight strengthened.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The responsibility for the Department's critical infrastructure protection and IT security are combined in the person of the IT Security Manager who reports to the CIO. Coordination with physical security is accomplished through a memorandum of agreement between the CIO and the Office of Security, which is responsible for physical security. Although progress has been made, the IG finds that security is not yet an integral component of the Department's business operations. They report that as a result fundamental responsibilities are not being carried out, including assessing risks to IT assets, determining security needs, promoting security awareness, and evaluating the effectiveness of security control policy.

13. ***Department methods to ensure contractor services are secure.***
    Contractors are subjected to security investigations and their work must be part of the review process for all systems. The IT Security Manager reviews functions out-sourced by the Department. A weakness identified by the IG was that neither the Federal Acquisition Regulations nor the Department's own acquisition policies provide the necessary guidance to ensure Commerce contracts contain provisions for security safeguards. The Department now reports sending a memorandum to all contracting officers emphasizing the importance of this area. The Department should use their plan of action and milestones to track progress in this area. OMB is working with the agencies to address this acquisition issue.

Department of Defense

1. ***Security funding.***
   The Department of Defense has reported planned FY 2002 funding for IT security and critical infrastructure protection of $1.77B, over twice all other departments and agencies combined budgets. This funding level comprises 7.5% of their total planned IT portfolio of $23.6B. The Department's total IT portfolio is roughly equal to all other departments and agencies combined.

2. ***Number of programs reviewed.***
   The Department maintains an "IT Registry Database of Systems" that lists over 3,700 systems,[1] each of which has a designated function and a manager. From this registry a statistical sample of 560 classified and unclassified systems were selected for

[1] Required by Public Law 106-398, title VIII; subtitle B, "Information Technology", section 811, "Acquisition and Management of Information Technology".

review. The DOD IG, in collaboration with the Army and Air Force audit agencies reviewed 90 major applications from a total population of 4,939 applications.

3. ***Review and independent evaluation methodology.***
The Department has formally established an Integrated Process Team that develops IT security review methodology guidance for Department components (bureaus, branches and agencies). The components provide assessment data for this report and the team was responsible for aggregating this information into an "assessment of assessments" to meet the Security Act reporting requirements. The Department used a combination of methodologies to develop a matrix of standard reporting elements. These elements were based on the NIST self-assessment guide, the Department of Defense Information Technology Computer Security and Accreditation Process, and other Department assessment vehicles. These methods were applied to the sample of 560 systems taken from the Department's IT registry. The IG's primary evaluation methodology was to identify which of the applications in their sample were certified and had designated security personnel. This was augmented by reviewing prior Department, IG, and GAO reports for information relating to the questions asked in the OMB reporting guidance.

4. ***Material weaknesses.***
The Department identified cumbersome IT management processes and outdated IT policies as material weaknesses in their IT security program. The rigorous, long and deliberate management processes that account for risk, resources, and customer impacts, can take more than 12 months to develop and coordinate. As a result, the Department is having difficulty implementing policies that are relevant in a rapidly changing IT environment. The Department plans to address this deficiency by issuing guidance memorandums under the Deputy Secretary's signature that are developed in weeks, but require frequent updates. The widespread existence of outdated policies is attributed to the recent and rapid evolution from isolated mainframe computers to networked desktop systems. The traditional approach of relying on general reviews during the budget cycle are no longer adequate to ensure IT security for the new systems whose number of vulnerabilities and severity of threats have increased dramatically. Due to the size and complexity of the Department's IT systems it is not surprising that at an application and system level the IG was able to discover weaknesses in virtually every area of IT security. For specific applications, systems and networks they found weaknesses in access controls, contingency planning, documentation, security awareness training, security design and implementation, and management controls among other deficiencies. The Department appears to be making significant progress in their development and implementation of and IT security program, but serious weaknesses persist and work remains to be done.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans, and tested controls.***
The Department's report does not identify the measures of performance used to ensure officials have assessed risk, determined security levels, maintained plans and

tested controls, nor does it provide any examples of how the Department has performed in these categories. The report indicates that measures of performance are documented in the "Department of Defense Instruction 5200.40," but no examples are given. The Department asserts that this instruction provides an oversight mechanism to ensure the identification of appropriate information to certify and maintain each program's security. The report goes on to describe four phases (definition, verification, validation, and monitoring) of mandatory activities used for the certification process. However the IG found that the Department had not fully implemented these security policies as evidenced by 60% of the application reviewed lacking certifications. The IG attributed the failure to implement these policies to unclear definition of security parameter and responsibilities, compounded by limited Department level and component head oversight and the practice of approving different organization to develop, operate and use IT applications. The IG also noted that while the Army had developed some measures of performance, they only applied to one of the information security categories in this area (testing), and in 79% of the Air Force applications evaluated, no performance was measured in any of the categories. The Air Force indicated that this situation applied to legacy systems, and has been corrected for new installations, but did not provide supporting data.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The report describes several specific areas where the Department is performing IT security practices intended to ensure the effectiveness of their program, but fails to give examples of performance measures, or actual performance in these areas. The Department states that it is impractical to specify measures of performance that relate to each program, however they do verify that all security patches have been added correctly to a system. For the performance of the special IT teams employed to attack systems to validate their safeguards, a performance measure could be the percentage of attacks that were successful. The absence of specific Department level measures of performance will hamper the Secretary's ability to oversee and ensure the CIO is adequately maintaining a Department-wide IT security program. The IG found that although Department of Defense Directive 5200.28 assigns oversight of policy implementation to the Assistant Secretary (Command Control, Communication, and Intelligence), and responsibility for implementation to the component heads, mechanisms have not been established to provide oversight or comprehensively measure compliance. The IG also found that although the Assistant Secretary established an integrated process team to evaluate and consolidate data to report the Departments IT security posture, they were unable to develop a plan that would consistently apply information security requirements across all Department systems and networks.

7. ***How the agency ensures employees are sufficiently trained.***

   The Department describes the most comprehensive training program and processes of any Federal department or agency. Their policies mandate annual IT security awareness training for their 3.4 million military and civilian employees, specialized

training for employees with significant IT security responsibilities, and certification of all users before allowing access to IT networks. They have established a Human Resources Development Functional Area to carry out personnel awareness training for information security, and use a variety of materials to accomplish this mission including video, computer, and web-based training. The Department reports disseminating over 127,000 videos and compact-disk training modules, and the Department's components have site licensees for commercial training software with vendors that have over 1600 titles. Employee awareness training is reported as being tracked, with up to 96% of the personnel receiving awareness training. The Department does not distinguish IT security training from other types of training, and is therefore unable to accurately identify costs, however $31.7M was budgeted, or roughly $10 per employee. The Department does not report how many of their employees were determined to require awareness or special security training, nor did they give any specifics about how many employees received specialized training, or the related cost. The Army Audit Agency provided the only finding in this area which was that the Army identified 14,000 information security specialist, of which about half were trained in FY 2000, with a goal of finishing the training in FY 2001.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department has a fully functional and effective incident response capability. Guidance and procedural frameworks for detecting, reporting, and sharing vulnerabilities are documented in the Department of Defense "Directive 8530.1, Computer Network Defense" and "Instruction 8530.2, Support to Computer Network Defense." A succinct summary of the criteria for reportable incidents, and the reporting process used within the Department and externally with national incident response coordinators, are provided in the report. The report also contains meaningful performance measures and actual results, e.g. 29,281 reportable incidents of which 384 resulted in unauthorized access. Although there is always room for improvement, the ability to defend against 98.5% of the cyber attacks is certainly good performance. The IG finding that the 384 unauthorized assesses resulted in 194 investigations leading to 24 criminal indictments, and ending in 18 convictions, provides a sense of the impact caused by the vulnerabilities. The IG estimated the monetary recoveries and cost avoidance from the investigation to be $2.9M. The Department of Defense incident detection, handling, and vulnerability sharing capability are the best among all Federal departments and agencies.

9. ***Department integration of security and capital planning.***
The Department stated that although security requirements and cost are reported annually in various budget documents, the Department was unable to provide information on whether IT security requirements and costs were identified on capital asset plans submitted to OMB. However the report does describe the investment control process they use to integrate IT security with their capital planning. The Assistant Secretary of Defense (Command Control, Communication, and Intelligence) as the designated CIO, with five deputies collaborate to ensure IT security is integrated with investments of IT systems. The Joint Requirements Oversight Council, which is comprised of representatives from the Office of the

Secretary and Department components, reviews major new acquisitions for compliance with integration of information assurance before they are allowed to proceed to the next stage. During the programming phase the Office of the Secretary directs an information assurance Program Objective Memorandum Issues Team to review implementation plans and makes recommendations as needed to assure IT security integration. During the budget phase Department component managers are required to specifically break out resources related to information assurance. The Department currently devotes 60-75% of their information assurance resources to their Information Systems Security Program, which is subject to annual review.

10. Critical asset prioritization and protection methodologies.

The report states that there is no department-wide methodology to identify and prioritize critical assets, or their dependencies on key external systems, in order to protect them within its enterprise architecture. Methodologies and capabilities that do exist vary widely across individual Department components, and are tailored to meet their specific needs. The Department did not discuss implementation of a department-wide methodology, or the adoption of an existing methodology such as Project Matrix that is being used by other Federal departments and agencies to perform this function. While this approach is effective for one Department, Project Matrix compiles the data from all agencies to support gap analysis across the government's enterprise. Given the considerable interaction between the Department of Defense and most other agencies, OMB will discuss with the Department an integration of their process with Project Matrix. The IG found that several of the Department's programs designed to protect critical assets were not required to identify or prioritize assets within the enterprise architecture. The IG observed that the Department has in place an information technology registry of over 3700 critical assets, but found that not all assets are registered. For a limited sample of 90 items reviewed by the IG, Army and Air Force audit agencies, only 21 were listed on the registry. The IG also noted that they did not review the overall effectiveness or completeness of the IT registry.

11. 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 report claims that standardized information assurance metrics are set fourth in the "Chairman of the Joint Chiefs of Staff Instruction, 6510.04, Information Assurance readiness Metrics." However the instruction is in review and no specific examples of the metrics are given. The only examples of measures of performance provided in the report are system security evaluations; operational assessments of a system's usefulness; and the number of certified system administrators. No actual performance data is given, instead the Department focused on policy and guidance that was issued for information assurance. Although the Department did not identify it as a performance measure, the IG found that in their review sample of 1,365 applications, 60% were not certified or accredited. The IG also reported that the CIO stated "it had several vehicles in place to assess information assurance, but did not have a way to evaluate and consolidate information assurance data to report the [Department] information security posture." The IG observed, "Without the means of evaluating

and consolidation data, [the Department] could not measure performance of information security throughout a system's life cycle."

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The report indicates the Critical Infrastructure Protection Plan documents the processes that ultimately ensure the reliability of physical and information infrastructures. Responsibility for critical infrastructure protection, as well as Information Security, and Information Assurance is assigned to the Deputy Assistant Secretary of Defense (Security and Information Operations), who is also the senior policy official for information, physical, personnel, and operational security programs. The coordination of cyber and physical security for assets owned and/or operated by a Department component are the responsibility of the component. The report does not provide specifics on how the components integrate the various security elements of their assets other than to state that risk assessments are conducted after assets are identified. This is intended to provide asset owners with a catalyst for vulnerability mitigation, minimizing operational impacts, and development of risk management protocols.

13. ***Department methods to ensure contractor services are secure.***
    The Department employs a variety of methods to safeguard the security of contractor provided IT services. The Department reports that all Administrative Contract Officers must include specific language on contractor security procedures in every contract. Some examples given in the report of material covered in these sections are; safeguarding classified information, procedures for securing telecommunications, and control of government personnel work product. The Department also relies on investigations, audits, and background screening and training for contract personnel. The IG cited several examples of security breaches in contractor provided services, most notably in the area of contractors, including foreign nationals, who were granted access to systems without appropriate background investigations. Although the IG was able to relate many examples of compromised contractor IT security, with a work force in the hundreds of thousands, without some sense of the percentage of the work force affected, it is difficult to ascertain from the IG's report the severity of the problem. The IG's findings show that there is need for improvement in this area, but overall the Department is stronger in this area that most other Federal departments and agencies.

Department of Education

1. ***Security funding.***
   The Department reports planned FY 2002 funding for IT security and critical infrastructure protection of $11.5M. This level of funding comprises 2.0% of their total planned IT portfolio of $575M.

2. ***Number of programs reviewed.***
   The Department reports reviewing all of their 104 major systems including 18 characterized as mission critical. Few other agencies matched Education's 100% coverage of major systems for their annual report.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide to review their systems. In addition to the NIST guide, which includes requirements of OMB policies and other NIST security guidance, they developed a supplemental survey to capture other information needed to comply with Security Act reporting requirements. The IG used the GAO's Federal Information System Controls Audit Manual as a guide for reviewing systems, as well as the results from reviews conducted by other parties.

4. ***Material weaknesses.***
   The Department identified material weaknesses and reports that it is correcting them, but not to the point of achieving a satisfactory level of performance. The IG notes that these weaknesses indicate that the Department is not in full compliance with the Security Act. Although the Department has undertaken a number of actions to address IT security issues, deficiencies still remain. The IG believes that the underlying cause for the significant weaknesses in IT security is the lack of a department-wide risk based security plan and program, supported by policy that ensures security training, incident reporting, integration with capital investments, and protection of critical assets.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   The Department has established policies and rules directing officials to give IT security a high priority, sufficient resources, and their personal attention. These policies will only bear fruit if the Department can maintain the necessary focus and leadership. The report does not reflect how the program officials will be motivated to ensure they have assessed risks, determined security levels, maintained plans, and tested controls; or how these policies will be enforced. The IG reports the Department is not carrying out these fundamental responsibilities. The Department reports they have security plans in place for 17 of 18 mission critical systems, but no explicit measures to ensure officials have assessed security risk, determined protection levels, or maintained up-to-date plans. They further state that only 25% of their systems have had overall risk determined, and only 42% of their systems have threats/vulnerabilities identified. The IG reports deficiencies in all seventeen IT security control areas identified by NIST as being critical for implementation of an adequate IT security program. They conclude that the Department is unable to provide a posture that sufficiently protects critical resources.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Department is defining measures of performance for their CIO and is considering measures for tracking and reporting. They expect a full metrics program to be in place in early 2002. OMB looks forward to reports on this program's effectiveness and will work with the Department to evaluate its potential use by other agencies. In the meantime, the IG reports that the Department does not have procedures implemented to ensure that the CIO effectively develops, implements and maintains security programs, and trains employees to promote security.

7. ***How the agency ensures employees are sufficiently trained.***
   The Department has established an annual training program, but as of the reporting period not all relevant staff have completed specialized IT security training. The Department reports that 98% of their 5000 employees received awareness training, costing $50,000, or $10 per employee. However, the report does not mention to what extent the specialized training is incomplete. Despite longstanding training requirements in the Computer Security Act of 1987, OMB policy, and NIST guidance, the Department of Education in the past has not devoted adequate attention to training. The IG reports that several Principal Offices were not aware of the requirements for IT security training and many individuals with significant security responsibilities, including both agency employees and contractors, had received no training.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   The Department does not have an effective incident response capability. Although some progress has been made in the last year and an Incident Handling Guide has been developed, it does not appear to be fully implemented, and no formal procedures exist for external reporting. Since only three of eighteen bureaus demonstrated an understanding of the need to communicate incidents to external entities, incident reporting needs improvement. Of the 39 incidents reported for the last twelve months, the IG observed that in some cases the incidents were not detected for 12 days. External reporting of one incident took an additional 12 days and did not include sufficient information to support analysis. The IG found that "the Department is unable to effectively detect, respond and report security incidents." Weak incident detection and reporting is a likely factor in the low number of incidents reported by the Department. The Department recognizes these shortcomings and plans program improvements, but provides no specifics.

9. ***Department integration of security and capital planning.***
   During the reporting period, the Department had not fully integrated security into its capital planning process. The Department appears to have corrected this problem by adding security funding to its FY 2003 budget submission for which OMB has commended the Department by separate communication. The IG noted that the guidance provided to program managers and the Board did not require specific

descriptions of system requirements or costs, which would be required to be fully compliant with the Security Act.

10. Critical asset prioritization and protection methodologies.

The Department reports that it has identified its mission and critical infrastructure using a contractor developed methodology. Discrepancies exist between the critical assets identified by the bureaus and the Department, but work is underway to resolve the differences.

The Department reports that is it is currently in the process of assessing the risks to and vulnerabilities of its critical assets. This information will be used to develop findings and recommendations. The IG reports that the Department's efforts in this area are deficient in that it did not follow its own methodology and it did not identify essential programs, services, and interdependencies and thus the inventory of critical assets is questionable. Accordingly, the Department may not be able to determine an adequate level of protection for its critical assets. The Department indicates confidence in successfully identifying their mission critical infrastructure and reports it will revisit the its identification of essential assets.

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

Currently the Department does not use specific measures of performance to ensure that the IT security plan is actually practiced. This is primarily due to the lack of a formalized and integrated approach for security life cycle management. The IG report states that the Department's System Development Life Cycle methodology makes no reference to security considerations during the development process. Furthermore, the Department's report does not explain how this situation will be rectified to comply with OMB guidance and the Security Act.

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

The Department uses two documents, its IT Security Plan and Critical Infrastructure Protection Plan, to set forth all necessary security measures in the Department. They and their IG both recognize the need to improve the process to better integrate cyber and physical security, and the protection of the Department's mission critical infrastructure. At present, integration is complicated by differences in risk ratings for a given asset depending on whether the list was prepared for Presidential Decision Directive 63, "Critical Infrastructure Protection" or Security Act purposes.

13. Department methods to ensure contractor services are secure.

The Department took steps last June to build IT security clauses into their external contracts and appended them to requests for proposals. The IG reports that the Department relies primarily on independent evaluations and reviews to determine if contractors are meeting OMB policy and NIST guidance. A weakness identified by the IG was that the Department's IT security policy lacks specific guidance for

ensuring that contracts include appropriate language to ensure contractor provided services meet OMB policy and Security Act requirements.

Department of Energy

1. ***Security funding.***
   The Department of Energy reports planned FY 2002 finding IT security and critical infrastructure protection of $109M. This funding level comprises 9.4% of their total planned IT portfolio of $1.15B.

2. ***Number of programs reviewed.***
   The Department reports reviewing eight Department level cyber-security programs. The Security Act and OMB reporting guidance require a review of all systems and programs. Their IG reported evaluating all program elements at twenty-four Department sites, but did not indicate how many site-specific programs or systems were included.

3. ***Review and independent evaluation methodology.***
   Energy uses a combination of policies, procedures, regulatory requirements, audits, and input from internal organizations. Their Office of Independent Oversight conducts regular assessments at levels appropriate to the systems under review, including remote scanning and penetration testing to identify vulnerabilities. It also evaluated whether site programs are meeting security objectives. The IG noted that the Department did not develop a specific template, or use other available methodologies recommended by OMB, as an aid for reviewing their information technology systems. As a result the assessments varied greatly in scope, areas reviewed, and system specific risk assessments.

4. ***Material weaknesses.***
   Energy has a history of weaknesses in their security program and for individual systems and has not fully implemented its IT management controls. They report that they are aware that material weaknesses have been identified. Their IG characterizes weakness in information security as impairing the Department's ability to protect their systems. The IG cites a number of underlying causes for the weaknesses in IT security including poor incident reporting, contingency planning, and management of intrusion threats.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   In FY 2001, the Department established uniform security metrics for all internal organizations to promote a comprehensive risk management process. They report approving 87 security program plans, but do not report how many programs or systems have yet to be approved. The Department reports that policy identifies line managers as responsible for accepting residual risks, but not how these policies are enforced or how program officials are motivated to ensure they have assessed risks

properly, determined appropriate security levels, maintained their plans, and tested controls. The IG reports the Department is not carrying out these fundamental responsibilities and state that only 50% of the systems evaluated have had risks and vulnerabilities assessed. They question whether the Department has the management tools in place to protect its critical systems. The Department must ensure that responsible officials are provided the tools to perform their jobs and be measured and held accountable for their performance.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The CIO manages security primarily through monitoring the Department's security program measures of performance. These measures include the number of security plans approved, incident reports, and promulgation of training. The Department reports that monitoring of these measures of performance, along with reviews and established policies are used to implement the program, but apparently the CIO lacks the authority or means to enforce the rules to ensure a secure program. The IG asserts that the CIO is not actively engaged in monitoring assessment activities and does not review programmatic level results to determine whether efforts are on track. The IG maintains that the Department lacks specific focused measures of performance for gauging the effectiveness of the cyber security program. The IG reports that the Department does not have procedures implemented to ensure that the CIO effectively develops, implements and maintains security programs, and trains employees to promote security, nor does it provide the CIO the authority or tools to accomplish this assignment.

7. ***How the agency ensures employees are sufficiently trained.***
   The Department has established annual training programs, but reporting was incomplete in this area. While the resources devoted to training are not uniform across all program and field offices, the Department pointed out that more resources are required for more sensitive programs of the Department's mission areas. The Department reports that at least $2.5M of the $72.6M security budget was spent on training. They submitted a representative sample of staff and training budgets accounting for $1.5M of the total. They indicated a total work force in excess of 117,000 with at least 2,000 categorized as systems administrators/specialists. For the offices that reported, FY2001 security training costs were approximately $250 for each key system administrator and averaged less than $10 per employee for security awareness training. The IG reported that many operating units exhibited weaknesses in IT security awareness and they could not identify who had received training or what it cost to provide the training.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   The effectiveness of Department's incident response capability is mixed and they recognize that improvement is needed. Some progress was made over the past year including an enhanced incident warning and reporting manual. Incidents per attempted intrusions have declined from 10% to 5%. The IG finds that reporting

needs improvement as less than 5% of reporting sites report all significant cyber-security incidents. Aggressive actions that enforce accountability at all levels will be required to mitigate the current problems.

9. ***Department integration of security and capital planning.***
   The Department reports that it uses their CIO's Software Engineering Methodology to integrate security into its capital planning process, however it did not report security costs on its budget submission for FY 2002 and does not expect full compliance until the FY 2004 budget cycle. The IG reported that since the Department does not separately report security requirements, the IG could not determine the extent that security is integrated into the capital planning process. OMB is working with all agencies to improve this process.

10. ***Critical asset prioritization and protection methodologies.***
    The Department was an early user of Project Matrix and continues to be a leader in this asset identification and prioritization effort. However, the IG feels that the Department has been slow to develop a baseline asset inventory, which is currently incomplete. Many offices within the Department are concerned that the inventories do not accurately reflect the prioritization of the assets and that the Department has not provided specific guidance to permit consistent prioritization.

11. ***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 uses extensive reviews to determine if their organizations are compliant with cyber-security plans, but the IG reports that they do not use specific measures of performance to ensure that the IT security plan is practiced. The Department makes reference to requirements imposed on organizations as a means to ensure the protection of IT systems, but does not indicate the management practices employed to ensure effective implementation of the requirements. The IG states that while the Department is developing a system development life cycle methodology, it has not reached this goal. While such a methodology is important, it will have limited effect without the appropriate management tools to ensure that plans are implemented, tested and maintained.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department reports that it has a formal approach to integrate critical infrastructure protection and IT security and has issued policy documents that establish a risk based approach to protection of critical assets. By using the prioritized asset inventory identified by Project Matrix, the Department believes that the approach can be extended to include physical assets. The CIO is in the process of developing a formal program that integrates cyber and physical security. Although progress has been made, the IG finds that security is not yet an integral component of the Department's business operations. They report that the lack of knowledge of fundamental aspects of the security programs, including assessing risk to IT assets, determining security needs, understanding threats, and identification of critical

infrastructure detracts from the Department's ability to effectively integrate security protection measures.

13. ***Department methods to ensure contractor services are secure.***
Contractors are subjected to security investigations and their work must be part of the review process for all systems. The contracted work force performs a substantial amount of the Department's functions and accordingly carries significant responsibility. The Department essentially applies the same oversight to the contractor staff as they do for the Federal employees, however the IG points out weaknesses in this area as well.

Environmental Protection Agency

1. ***Security funding.***
EPA reports planned FY 2002 funding for IT security and critical infrastructure protection at $9.2M. This level of funding comprises 2.5% of their total planned FY 2002 IT portfolio of $361M.

2. ***Number of programs reviewed.***
The Agency reports an inventory of 95 major applications and 94 general support systems, but indicate that only 44% of those systems were evaluated. The Security Act and OMB reporting guidance required a review of all programs and systems. The IG was aided in their review efforts by their analysis of prior Agency, GAO, and independent contractor assessment reports, and focused their efforts on assessing the implementation of 26 prior GAO recommendations.

3. ***Review and independent evaluation methodology.***
The methodology used by the Agency is a combination of policies, procedures, regulatory requirements, audits, and input from Agency organizations. They conduct regular assessments at levels appropriate to the systems under review, including penetration testing to identify vulnerabilities, and whether programs are meeting security objectives. The report cites developing and using its own risk-based methodology that considers technical, operational, and managerial issues. The Agency notes that future reviews will be based on the NIST self-assessment guide.

4. ***Material weaknesses.***
Despite a history of weaknesses in their security program and security for individual systems, the Agency appears to still be in the mode of developing and evolving security plans. While planning is essential, this has been an explicit statutory requirement since the enactment of the Computer Security Act of 1987 and by now, the Agency should be executing reliable established processes including implementing and testing security plans and controls and assessing security performance. The Agency has not been effective implementing its IT management controls and has yet to establish an Agency-wide system that adequately addresses fundamental IT security issues relating to planning, reviews, testing, training, or

integration with physical security. Their report to OMB shows that the Agency is aware that material weaknesses have been identified and provides milestones for corrective actions along with implementation status. Their IG characterizes weaknesses in information security as impairing their ability to protect their systems. The IG cites a number of underlying causes for the weaknesses in IT security including weak or inadequate: risk assessments, incident handling, capital planning, enterprise architecture, infrastructure protection methodology, and security program oversight.

5. ***Measures of performance used by the Agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency reports that it has established measures of performance, and reports actual performances for assessing risk, determining appropriate levels of security, maintaining security plans, and testing security controls. The Agency has prioritized and conducted risk assessments on the most critical 37 of their 189 major applications and information systems. Of the 189, 92% have had the sensitivity level of information categorized, 89% have had their plans updated in the last three years, and 44% have actually been evaluated. Some penetration and vulnerability testing on the applications and systems revealed poor documentation and account management, standards not implemented, and non-compliance with Agency policies. The serious problems were addressed quickly, and the remainder scheduled for correction in 120 days. The number and type of vulnerabilities discovered does cause concern over the potential vulnerabilities within the 55% of applications/systems that were not evaluated. Policies and rules directing officials to give IT security a high priority are in place, however, it is not clear how the Agency will motivate program officials to ensure they have assessed risks, determined security levels, maintained plans, and tested controls; or how these policies will be enforced. The IG reports the Agency was still in the process of developing their measures of performance when the IG fieldwork was being conducted, and was unable to evaluate the appropriateness of the Agency's measures or report on their adequacy.

6. ***Measures of performance used by the Agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Agency reports that the CIO manages security primarily by monitoring the EPA's Technical Information Security staff's project management function to track the security program's measures of performance. These measures include the number of risk assessments/security plans in place, reviewing security controls and incident logs, and the number of fixes implemented. The report goes on to say that the CIO has broad authority to protect the telecommunication network, but does not indicate how this relates to maintaining the overall security program. Since the CIO is still promulgating guidelines that support this policy, the report does not contain specifics on how the CIO's authority will be translated into an assurance that an effective program will be implemented. The IG reports the Agency was still in the process of developing their measures of performance when the IG fieldwork was being conducted, and was unable to evaluate the appropriateness of the Agency's measures

or report on their adequacy. As a result the IG cannot confirm that the Agency has procedures implemented to ensure that the CIO effectively develops, implements, and maintains security programs, trains employees to promote security, and is provided the authority/tools to accomplish this assignment.

7. ***How the Agency ensures employees are sufficiently trained.***
   EPA reports having established annual training programs, but the reporting of the resources was incomplete at the conclusion of the IG's fieldwork. This made it difficult for the IG to assess the adequacy of the Agency's security training. The Agency now reports that some $925,000 of their $10.9M security budget was spent on training. FY 2001 data reflects 530 sessions of specialized security training in seven categories were given to the technical staff, costing approximately $1400 per session. The report did not show how many different individuals received training or how many of the 675 technical staff required training. The Agency also reports spending $100,000 for web-based security awareness training, with 15,500 of the Agency's 18,000 having taken the course during the reporting period. The IG found that missing and incomplete data made the training numbers unreliable and points to the difficulty in identifying which employees have received training or the costs to provide it.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
   EPA does not have a fully effective incident response capability, although some progress has been made in the last year. The Agency reports that it is enhancing its incident warning and reporting, but does not appear to have uniform practices for internal or external reporting. Over a 16-month period, the Agency reports a total of 1,430 incidents, with 180 reported to the Agency's Technical Support Center. Depending on the region or office, the number of reported incidents varied widely indicating a lack of consistency across the Agency. This inconsistent reporting can adversely affect other entities (e.g., GSA's Federal Computer Incident Response Center and the FBI's National Infrastructure Protection Center) that rely on this data for analysis and broad warning to other agencies. The lack of uniform guidance in defining what constitutes an incident, or the establishment of reliable detection methods, may be a factor in the wide range of incidents reported. EPA is aware of these shortcomings and is making an effort to correct them by enhancing their security program policy guidance. The Agency reports approving a new Agency-wide incident handling model, but the IG found that no implementation schedule has been developed, nor have significant resources been dedicated to achieving the goal. Based on past performance, greater management oversight, and aggressive actions that enforce accountability at all levels, will be required to mitigate the current problems.

9. ***Agency integration of security and capital planning.***
   EPA reports that it is integrating information security into its capital planning and investment control process by requiring that proposals for new systems demonstrate the existence of a security plan that includes requirements and milestones. They also state that security costs were reported in the FY 2002 capital asset plans included in

their budget submission to OMB. However, the IG contradicts the Agency's statement with the finding that the Agency "has not consistently integrated security into its capital planning and investment control process." They note that some 30% of the 47 IT project proposals that they reviewed lacked approved security plans. The IG goes on to state that although cost data was included in the proposals (last fall, OMB worked with the Agency to correct deficiencies), the Agency lacks an accounting system that would enable them to substantiate the project costs. The Agency and the IG are resolving the discrepancies in this area.

10. Critical asset prioritization and protection methodologies.

EPA reports that they have developed a Critical Infrastructure Protection Plan. The first step identified critical assets and they refer to five critical facilities and 16 critical locations. They indicate that they plan to participate in Project Matrix in the future. The IG finds that the Agency "management has not identified, prioritized, or otherwise specified a methodology for protecting critical assets under its enterprise architecture plan." EPA has deferred that component of its architecture plan until a later date. Until completion of this process, including a complete identification of critical assets and their internal and external interdependencies, EPA is not in position to adequately prioritize protection requirements.

11. Measures of performance used by agency head to ensure practice of security plan.

Only 41% of the Agency's major applications and systems have lifecycle security documentation and the Agency has not demonstrated any management practices used to ensure the implementation of the plans that do exist. The current status of the Agency with regard to their practice of security plans did not allow the IG to offer any significant findings other than to comment that the Agency does not periodically validate whether regional and program offices actually implement policy requirements. It is important for the Agency to quickly establish and implement management tools to evaluate whether Agency officials are fulfilling their security responsibilities.

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

EPA reports that its physical and cyber programs are integrated and refers to security program documentation and vulnerability assessment procedures as support. The IG reports that better integration is needed and found that management's inability to describe a methodology to identify and prioritize assets may result in misapplied security resources. Although not an integration issue, the IG also noted here that two major IT infrastructure projects did not have required security plans. The Agency agrees that better integration is needed.

13. Agency methods to ensure contractor services are secure.

EPA uses three processes to ensure the security of contractor provided services: background investigations, contract language, and audits. The Agency currently has a significant backlog of security checks. The IG finds that across the Agency there is not a process to ensure contractor services are secure and they emphasize that its

absence is a key contributor to the weaknesses of the security program. They go on to state that they have advised the Agency for several years to establish a security program with strong oversight to address risks and secure valuable data.

Federal Emergency Management Agency

1. ***Security funding.***
   FEMA plans FY 2002 funding for IT security and critical infrastructure protection of $2.9M. This level of funding comprises 1.8% of their total planned IT portfolio of $166M.

2. ***Number of programs reviewed.***
   The Agency reports an inventory of approximately 50 major applications and systems. Of these, 13 were identified in their critical infrastructure protection plan and are referenced in the report as the focus of the review. The Agency also reports evaluating six other systems including three classified systems. Neither the Agency nor their IG states specifically how many of the systems not evaluated were mission critical. The Security Act and OMB's reporting guidance required a review of all programs and systems.

3. ***Review and independent evaluation methodology.***
   The Agency employed an independent contractor to evaluate their systems and develop a baseline for future audits and evaluations. The IG confirms that the methodology used was appropriate. It is reported to contain suitable elements for a methodology, including identifying architecture and vulnerabilities, reviewing policies, controls, and implementation. The Agency also had their IT security program assessed by the NIST Computer Security Expert Assist Team, a good choice.

4. ***Material weaknesses.***
   The Agency has begun to implement its restructured IT management controls in the last several months and has yet to realize the expected benefits. This is a good approach, but FEMA must follow through aggressively. Material weaknesses have been identified and are being corrected. The Agency still has weaknesses in documentation of training received by their employees and contractors, and in assuring the reliability of their work force with background checks/investigations. The IG recommends better coordination between the Human Resources Division that tracks training and the IT Security Office responsible for monitoring IT security training. Due to funding priorities within the Agency there is a backlog of over 1000 security clearances that is a consequence of a $500,000 shortfall. The Agency reports that they consider protection of information systems a higher priority than security documentation and verification of employee integrity, but they do not address IT security funding priorities in the larger context of all Agency activities.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   FEMA has made significant improvements in their understanding of IT security, but they have yet to have a fully functional program. Although their report indicates program officials have a high awareness of the issues relating to IT security risk assessments, determining security levels, planning and controls, the Agency has yet to devote the resources to implement agency-wide risk assessments or finalize plans for all of their critical systems. The IG finds that the Agency Information Resource Management and Procedure Directive is outdated. They further note that the Agency recognizes this and is planning to update the directive, but have not yet done so. The report indicates there have been "recent funding increases for the system security program" which is expected to improve the program.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   FEMA reports that it has chosen to interpret "measure" to mean a "planned action" as opposed to a "measurement," i.e., actual performance. Consequently the measures of performance for the CIO are given in the form of what will be done as opposed to actual accomplishments. For example, there are plans to issue policy, inform officials of their responsibilities, and review system plans, but there is no indication of what standards are used to determine the effectiveness of the CIO's actions.

7. ***How the Agency ensures employees are sufficiently trained.***
   The Agency has established annual training programs, but the reporting did not make clear the relationship between the types of training being given and the requirements for a sufficiently trained staff. The Agency reports that $56,500 of their $2.9M security budget was spent on specialized security training for 248 of their 5,700 employees, but does not indicate how many employees required training, but didn't receive it. The report also notes that 110 additional training sessions were conducted through the SANS (Systems Administration, Networking, and Security) Institute, however the IG found that this was insufficient to meet the demand for advanced IT security training. For security awareness training, the Agency is relying on distribution of news articles and emails to computer users. They plan to include awareness briefings as part of new employee orientation and are considering web-based training. Web-based training is an effective approach especially if they can take advantage of awareness training programs that have been implemented by other agencies.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
   FEMA reports making progress over the last year in incident information sharing and is in the process of implementing a full-time, round-the-clock incident response capability. They state that last year only two incidents were reported. The Agency does not report incidents to the GSA's Federal Computer Incident Response Center or the FBI's National Infrastructure Protection Center unless it exceeds a $5000 damage threshold. The Agency is not sharing trend information on lesser events. This type of

information can be an important factor in the analysis of potential threats and external reporting and information sharing is required by both the Security Act and OMB policy. The Agency expresses confidence in their firewall protections, but the IG does not. Weak detection capabilities are a likely factor in the low number of incidents reported. The Agency reports plans to quickly improve its ability to defend against, detect, and report incidents. Sustained management attention and resources are necessary to effectively implement this program.

9. ***Agency integration of security and capital planning.***
   The Agency reports that that they addressed security requirements in their FY 2002 capital asset planning but did not identify costs. They recognize that cost reporting is inconsistent and plan to correct this issue. The IG is planning an audit, but lacking this information in the FY 2002 budget materials, was not able to comment on this requirement. Without fully understanding security requirements and their associated costs, it is difficult to identify the amount of resources necessary to correct problems.

10. ***Critical asset prioritization and protection methodologies.***
    The Agency has begun a Project Matrix review to identify and prioritize critical Agency infrastructures and interdependencies between key systems. The IG feels that the Agency has been slow to develop a baseline asset inventory and is concerned that the Agency is using this methodology only to identify assets that impact "national security" and the "national economy" and may neglect systems essential to the Agency's mission. At this point, the Agency is still in the early stages of identifying and prioritizing the Agency's critical assets.

11. ***Measures of performance used by the agency head to ensure practice of security plan.***
    In their report the Agency has chosen to interpret "measure" to mean a "planned action" as opposed to a "metric," which is the intended in the context of these reports. As a result, the measures of performance used by the Director of the Agency are given in the form of what will be done as opposed to actual accomplishments. For example, the report states that the FEMA Director reviews the security program and requires plans including resource requirements, but does not indicate what standards he applies to determine if the security plan is practiced throughout the lifecycle of each system. The IG found that "the CIO should develop measures of performance relating to the cost, schedule, and security performance of each system to enhance accountability." The IG further states the need for a system security accreditation process and goals to form the basis for performance measures. To ensure compliance with the Security Act, program improvement, and sustained effective program management, it is critical to establish measures of performance.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The responsibility for the Agency's critical infrastructure protection and IT security are combined in the person of the Enterprise Security Manager. No mention is made in the report of how coordination with physical, and operational security programs is

accomplished, or who is responsible for physical security. This is a concern because effective integration of all aspects of security is vital to understanding threats and security needs. The IG briefly stated that integration of security is important, and observed that the Enterprise Security Manager was taking the lead for assuring information security.

13. ***Agency methods to ensure contractor services are secure.***
The Agency reports that contracting officer's technical representatives are responsible for ensuring that contract language and oversight of contractor provided services are secure. They also rely on external audits to verify contractor compliance. The Agency does not report on any methods used to determine the reliability of the contractor work force, such as background checks. The IG states that contract vehicles "should have very specific language as to the contractors' requirements," but does not indicate whether such language is used. The IG goes on to state that the Agency contracts should include requirements for contractors to provide evidence of an independent assessment.

General Services Administration

1. ***Security funding.***
The General Services Administration reports planned FY 2002 funding for IT security and critical infrastructure protection of $14.8M. This level of funding comprises 3.3% of their total planned FY 2002 IT portfolio of $455M.

2. ***Number of programs reviewed.***
GSA reports they conducted high-level reviews of all 42 major applications and systems within the Agency. The also performed more detailed self-assessments for nine of the systems in five of their seven staff offices/services. The Security Act and OMB guidance required a review of all agency programs and systems. The IG identified 36 systems as mission critical. Neither the Agency nor their IG states specifically how many of the systems were evaluated using the more detailed self-assessments were mission critical.

3. ***Review and independent evaluation methodology.***
The Agency reported using two methodologies to review IT security for their major systems and applications. The first is a high-level review that has been conducted for all 42 major and significant systems. It entails determining the status of the systems' risk-assessments, security plans, certification, testing and evaluation, and budget review. The second methodology is based on the NIST self-assessment guide, which covers seventeen control areas. OMB recommended that all agencies use this approach. The IG did not describe their methodology, but they do refer to NIST requirements on several occasions implying that it was used in some way.

4. ***Material weaknesses.***
   Although the Agency has a history of IT security weaknesses, and their IG reported that a PriceWaterhouseCoopers LLP audit identified two "reportable conditions," the Agency did not report any material IT security weaknesses in this report. The "conditions" identified in the audit were the continuing need to improve security management oversight and improve development, implementation, and change controls over the Agency's system environment.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency has established and reports actual measures of performance for this topic. They indicate they have conducted reviews of 42 major or significant applications and information systems. Of these systems, 48% have had risk assessments, 62% have had their plans updated in the last three years, and 14% have received certification/accreditation. Testing of security controls has been evaluated on 2% of the 42 major application/systems. While GSA has made progress in defining and tracking performance measures, the low-level of actual performance, especially vulnerability testing, raises significant concerns about the Agency's effectiveness of management performance. The IG found in their review of seven information systems, similar patterns of partial compliance with IT security requirements and recommends the inclusion of testing and evaluation as part of the certification process. The IG also found that the Agency does not have an Agency-wide security plan with processes to ensure that established control techniques are followed nor have they identified the goals and milestones needed to measure improvement.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Agency reports that the CIO primarily monitors the Agency's security program performance by working through the IT Security Center of Expertise. The performance measures apply to assessing risk, planning, certification, testing, and the number of employees receiving training. The report describes in some detail the NIST self-assessment guide reviews for nine systems. The Agency is still in the early stages of applying this methodology and appears to be implementing it in an appropriate and systematic manner. Although the results show that they are not compliant with many of the Security Act's requirements, they are moving in the right direction. Two areas that need significant improvement are testing and evaluating systems to understand risks and verify the effectiveness of safeguards and developing mechanisms to enforce the consistent application of IT security policy and procedures across the Agency. The IG did not specifically address this topic in their submission.

7. ***How the Agency ensures employees are sufficiently trained.***
   The Agency is still in the process of developing a formalized Agency-wide IT security training program, and understands the need to track such a program. They report spending $285,800 on training, $5,000 of which was devoted to awareness

training for 70% of the 14,000-employee work force ($0.35 per person). The remainder was used for specialized training for managers and IT professionals. This professional training ranged from $150 to $2,700 per employee. The IG found that several gaps still exist in the training program. They include an assessment of the IT security knowledge needed by employees to do their job, a formal training curriculum, and a mechanism to track and evaluate training effectiveness. Of special concern to the IG were cases where successful training courses were mandatory for employees but not contractors, or were discontinued altogether. The IG also found that although the Agency is making progress training individuals with special IT security responsibilities, many do not have adequate training to perform their jobs.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
The Agency reports it has instituted policies and procedures coordinated through their IT Security Center of Expertise to serve as the foundation for their incident handling capability. The documented policies and procedures serve as a standard for bureaus to report incidents. Significant IT security incident information is shared with incident coordinating centers and with law enforcement agencies. The measures of performance used by the Agency for FY 2001 include incidents reported to GSA's Federal Computer Incident Response Center (10), number of hacks deflected (13,000), email scams reported (2), and email viruses filtered by the firewall (52,000). The IG found that although the Agency had established guidance for reporting and handling incidents, they are "silent on Agency-wide policies or procedures for the detection of security breaches as required by [the Security Act]."

9. ***Agency integration of security and capital planning.***
The Agency's methodology for its IT capital planning and investment process is the Information Technology Investment Portfolio System. Security requirements are integrated with capital planning when they are defined as part of the IT evaluation process. Security requirements and costs were not reported on every FY 2002 capital asset plan submitted to OMB. The IG found that security costs had been included for only 16 of 36 mission critical initiatives and only 30 of the 108 total IT projects. The Agency reported that 41 of 42 systems reviewed have reported security funding and provided an appendix to their report that lists FY 2001 and FY 2002 security funding for many systems. Although the Agency can identify security funding for many systems, the IG findings show that this information had not been incorporated in the IT Investment Portfolio System used to integrate security and capital planning. GSA has made much progress in this area, but more work remains. OMB is working with all agencies to improve integration and reporting in this area.

10. ***Critical asset prioritization and protection methodologies.***
The Agency has begun a Project Matrix review to identify and prioritize critical infrastructure, links, and interdependencies between key systems and applications. OMB has directed most large agencies to undertake a Matrix review. This first step focuses on critical assets as defined by Presidential Decision Directive-63, i.e., those impacting "national security" and the "national economy." To be complaint with the

Security Act and OMB policy, later stages must address those systems essential to the Agency's mission.

11. Measures of performance used by agency head to ensure security plan is practiced.

The Agency reports that it used essentially the same measures of performance for ensuring security plans are practiced throughout an IT system's lifecycle as those used to ensure program officials are assessing risk, determining security levels, maintaining plans and testing controls. As indicated in topic five above, out of 42 systems, 48% have had risk assessments, 62% have had their plans updated in the last three years, and 14% have undergone certification and accreditation. Testing of security controls has been evaluated on 2%. They also plan to track high-risk system vulnerabilities, but do not yet have data to measure performance. As mentioned previously, the low-level of actual performance, especially in regards to vulnerability testing, indicates that the Agency is not effectively managing security plan implementation. The IG assessment of seven information systems showed similar deficiencies and recommends the inclusion of testing and evaluation as part of the certification process. The IG also finds that GSA does not have an Agency-wide security plan with processes to ensure that established control techniques are followed, nor have they identified the goals and milestones needed to promote and measure improvement.

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

GSA integrates their IT, physical, and operational security with their critical infrastructure protection program by issuing policy and procedural guidance for all facets of security and by involving their IT Security Center of Expertise in day-to-day operations across the Agency. However, the IG reported "operational roles and responsibilities for implementing the Critical Infrastructure Protection Plan across [the Agency] have not been established and [the Agency's] Critical Infrastructure Assurance Office lacked operational and policy authority to direct IT security policies and procedures necessary to implement the plan."

13. Agency methods to ensure contractor services are secure.

The Agency states that security policy applies to all individuals they employ including contractors, associates, and consultants. The Agency reports that in addition to including specific IT security requirements in contract language, they also require logging of contractor network activities, conduct background investigations, and perform routine assessment checks of contractor activities. The assessments include penetration testing of systems to help determine whether vulnerabilities exist. Neither the Agency nor the IG provided information on the level of performance. However, other information indicated that only 2% of the 42 systems reviewed for this report had security controls tested and evaluated. Thus, while a review process may exist, implementation appears significantly lacking.

Department of Health and Human Services

1. ***Security funding.***
   The Department did not provide data on headquarters-level or department-wide spending but contained in the body of the report was funding information for each of their major operating divisions. To arrive at the requested information, OMB aggregated the Department's individual IT funding requests and estimated the Department's planned FY 2002 IT security and critical infrastructure protection spending to be $62M. This level of funding comprises 1.5% of the Department's total planned FY 2002 IT portfolio of $4.2B. OMB was unable from HHS reported data to judge the comprehensiveness of its estimate.

2. ***Number of programs reviewed.***
   The Department reports relying on approximately 900 systems for day-to-day operations, and reported that they reviewed a total of 56. The Security Act and OMB reporting guidance required a review of all agency programs and systems. The IG conducted independent evaluations of security practices in all 13 of the Department's major agencies and 11 operating divisions responsible for over 300 programs. The IG relied on the Critical Infrastructure Assurance Office Project Matrix report findings to down select to 28 out of 97 Department systems that were identified as critical systems.

3. ***Review and independent evaluation methodology.***
   The Department did not use (but says it is developing) a uniform Department-wide methodology to review the adequacy of IT security programs. They report, "most agencies conduct some form of IT security program reviews." They also report using the results of their Project Matrix review (an excellent starting point) and noted that their financial system audits include an evaluation of the security controls. The IG reported that their methodology included reviews of prior audits required by Presidential Decision Directive 63, "Critical Infrastructure Protection", financial information system audits, and supplementary audits designed to address specific issues raised in OMB's reporting guidance. Consistent with OMB's recommendation they focused on the control areas outlined in the GAO's Federal Information System Controls Audit Manual.

4. ***Material weaknesses.***
   The Department and the IG reported that one HHS agency "indicated it had an outstanding IT security program related material weakness," but did not indicate what the weakness was, or how it was going to be addressed. The IG found "numerous instances in which basic controls were lacking or inadequate." The IG cited the underlying causes for the deficiencies as an ineffective security program management structure, weaknesses in security program planning, management, and access controls.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The Department did not report "specific measures of performance" or "information on the actual performance" used by the agency to ensure that: 1) program officials have assessed risk, determined security levels, maintain security plans, and test controls; and 2) that the CIO has effectively implemented and maintained a Department-wide security program or ensured the training of employees with significant security responsibilities.

   The Department CIO reported much in the way of promising intentions and plans for the future and includes indications of good security in some of the agencies, but the focus of the this report, the questions asked in items five and six, and indeed the Security Act itself, is effective program management and actual performance. Sustained, effective, and measured program performance will promote the expansion of good security beyond localized elements.

   HHS does report having established standard Department-wide performance measures that will be implemented this fiscal year, certainly a good step. Historically, the Department has not had strong headquarters-level management control in this area. Ensuring compliance with these standards will require strong leadership.

   The IG reported more detail on actual performance. They found that all agencies had weaknesses related to entity-wide security programs and access controls. Eight of 13 agencies did not have an up-to-date security plan or an effective security management structure. Four had inappropriately permissive access controls. Eleven had weaknesses related to service continuity. Other deficiencies reported by the IG were that eight of agencies had not performed adequate risk assessments of all of their systems. Seven had not tested security controls or certified systems in accordance with OMB policy. Fourteen of the systems reviewed did not have security plans and another 10 only had draft plans that did not contain all the elements required by OMB policy. Six agencies did not regularly review audit logs for security violations, which permits intrusions to go undetected. Ten did not have contingency plans or had not tested them to see if they work, and six had inadequately trained staff and poor environmental controls to respond to emergencies.

   HHS as a Department is not compliant with this area of Security Act or OMB policy. As the Department's IG found, and as has been reported on a government-wide basis by GAO for a number of years, strong central management and oversight at the headquarters-level is essential for consistently adequate security program performance.

7. ***How the agency ensures employees are sufficiently trained.***
The Department provided no Department-wide training data. They indicated that most of their agencies "provide some sort of security training," but they did not report the amount, the types, or the cost of training. The body of the report included some information regarding employee training at the component agencies, but it was not sufficient to demonstrate an adequate agency or department-level program. No program performance data was provided. HHS did report the FY 2001 award of a contract to provide security awareness training to all HHS employees by July 2002.

The IG found that five of the thirteen operating divisions had not met this requirement. The Department's failure to sufficiently educate its work force hampers their ability to adequately protect IT resources and puts the Department's assets at risk. These deficiencies are especially troubling given that security training has been a statutory requirement since the Computer Security Act of 1987.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department reported issuing a new incident response policy in January 2001 and is in the process of establishing a department-wide incident response team. Potentially this will satisfy the Security Act requirements for sharing computer incident and vulnerability information. We look forward to actual performance data. The CIO advised that all agencies reported that they adhered to this policy and reported incidents to the IG Computer Crime Unit, the Department, and GSA's Federal Computer Incident Response Center. HHS failed to provide any of the information specifically requested by OMB on actual performance, such as intrusion attempts, incidents detected, averted, and reported.

Though some of the component agencies have institutionalized formal IT security incident response teams most have identified "virtual" incident handling teams that operate on an as-needed basis. Nevertheless, the IG judged that four of the thirteen bureaus lacked either the procedures or the trained staff to handle security incidents. Based on the current status and past performance aggressive and coordinated management attention is needed in this area before the Department meets the requirements of the Security Act and OMB policy.

9. ***Department integration of security and capital planning.***
The report indicates that all bureaus incorporate IT security in their capital planning process, including identifying threats to software development and considering IT security related costs in the business case analysis. They also report that all bureaus identify IT security costs in the capital asset plans included in their budget submission to OMB. The Department's cost tracking efforts are good and necessary to integrate IT security with capital planning. Although accounting for security investments does not guarantee an integrated program, it is an essential ingredient for management oversight. The Department commented that security funding has not kept pace with the growth in security concerns. Inasmuch as the Department and its program officials have control over how they allocate their resources, this issue should be

quickly resolved. OMB will assist the agency in doing so. The IG did not evaluate the investment review process and did not comment in this area.

10. ***Critical asset prioritization and protection methodologies.***
    The Department was an early adopter of Project Matrix developed by the Department of Commerce Critical Infrastructure Assurance Office. A Project Matrix review assists an agency in identifying and prioritizing their critical assets and identifies links and interdependencies within and outside an individual Department. Accurate identification and prioritization of critical assets is at the foundation of an effective IT security system. The Department has identified 97 critical assets from which 18 were designated as highly critical. In addition to this effort, the IG found that all bureaus had developed their own review process to update their critical asset lists. However the IG also found that four of the thirteen bureaus were unable to produce complete lists of their systems with critical and sensitivity classifications, indicating more work is required in this area.

11. ***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 report contains little valuable performance information. The IG reported that various methods were being used, or were planned, by most of the agencies, but there are no specifics on the actual performance.

    Similar to items five and six, above, there appears to have been little effort in the past at the Department-level to oversee the efforts of the agencies and thus the Department could have no assurance that IT security plans are being followed when in fact they exist.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department reports that the use of Project Matrix assists in this area as its methodology includes most all security disciplines. OMB agrees, but notes that the weak central management structure discussed above, introduces concerns.

13. ***Department methods to ensure contractor services are secure.***
    The Department states that most agencies have implemented IT security controls, but recognize that there is a need for improvement. The report does not identify the specific methods (e.g., audits or inspection) used by the Department to ensure that contractor provided services are adequately secure. Although no Department-wide practices are in place and the IG found that eight bureaus "had not taken sufficient measures to ensure contractor compliance through background checks," they did find various constructive methods being applied in several bureaus. These included instances of contract clauses that call for the definition of security requirements, Information Resource Management review of contracts, and requirements that off-site contractors provide their own security plans. These good practices fall short of an effective Department-wide program and HHS must work hard to meet the

requirements of the Security Act, the Federal Acquisition Regulation, and OMB policy.

Department of Housing and Urban Development

1. ***Security funding.***
   The Department of Housing and Urban Development reports planned FY 2002 funding for IT security and critical infrastructure protection of $9.6M. This level of funding comprises 2.6% of their total planned IT portfolio of $376M.

2. ***Number of programs reviewed.***
   The Department reports reviewing twenty-seven programs, with plans to review another ten in the near future, but does not explicitly identify the number of programs in the Department. Additionally they indicate that self-assessments have been performed on 70 of 200 systems. The Security Act and OMB reporting guidance required a review of all programs and systems.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide to review their IT systems. They have also developed criterion customized to the levels of risk appropriate for the reviews, and that is consistent with OMB policy and Presidential Decision Directive 63, "Critical Infrastructure Protection." The IG used generally accepted government auditing standards, including interviews, reviews of existing documentation, handbooks, budget reports, as well as the results from reviews conducted by other expert parties.

4. ***Material weaknesses.***
   Despite a history of reports highlighting weaknesses in their security program and security for individual systems, the Department still has serious weaknesses in virtually every aspect of their IT security program. Weaknesses are reported by the Department and the IG in risk assessment, mitigation and management; insufficient security planning and documentation; incident tracking and reporting; inadequate computer access controls to protect against intrusions; and ineffective IT security training. To the Department's credit they are able to understand and articulate their weaknesses. However, the fact remains that this Department continues to exhibit continued weaknesses in their IT security programs, and require significant improvements to meet the requirements of the Security Act.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   The IG finds that the "security program is not at the level of maturity where they define, gather, and report performance measures in this area." The Department reports that the CIO is attempting to correct this situation with plans to develop measures of performance consistent across all IT operating areas. This will include enforcement of the security program, ensuring awareness training, and reporting of

security violations. The lack of any measures of performance to determine whether officials are assessing risks, maintaining security plans and testing controls is a serious weakness and brings into question whether the Department can effectively manage an IT security program without these metrics.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The IG again finds that the "security program is not at the level of maturity where they define, gather, and report performance measures in this area." The Department reports that some performance metrics have been defined for the CIO, of which they give examples, however no information is given on the actual performance against these measures, as OMB requested. The definition of these measures is certainly an important first step, but fail to completely address the requirements of the Security Act. The lack of specific examples in the Department's report reinforces the IG assertion of an immature IT security program, and a possible lack of Department leadership in this area. It should be noted that although the Security Act reporting requirements are relatively recent, statutes have been in place for over a decade that require Departments to maintain effective IT security programs.

7. ***How the agency ensures employees are sufficiently trained.***
   The Department has policies in place that require appropriate levels of training for all employees prior to being granted access to computers. They also show a planned training budget for FY 2002 of $1.4M, which is approximately $140 per employee for their work force of 10,000. However they only report training 584 employees in FY 2001, and do not indicate how much was spent in the process. Of some concern is the data showing only nine System Administrators receiving training when the Department reports having over 200 significant IT systems. Despite specific training requirements in the Computer Security Act of 1987, the Department has not devoted adequate resources to training. This observation is supported by a small percentage of the work force receiving training, and is another indicator of the immaturity of the IT security program.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   The IG confirms that the CIO has implemented a draft policy for a Computer Incident Response Program. This plan proposes several enhancements to a department-wide incident response center that will bring it in closer compliance with Security Act requirements. This includes a 24 hours-a-day, seven-days-a-week presence, standard operating procedures to share information with established incident coordinating centers like GSA's Federal Computer Incident Response Center and the FBI's National Infrastructure Protection Center, and documenting threat information in security plans. The IG found that contrary to OMB guidance, the Department's IG was not included in the reporting process. These plans represent a significant improvement over their current ability to share information. A difficulty with the current situation is that the Department may be unable to effectively detect, respond and report security incidents. Weakness in the incident reporting system makes it

difficult to know when an incident has occurred, and may be a factor in only two incidents being reported in FY 2001. The Department seems to be aware of these shortcomings and is making an effort to correct the situation by further enhancing their program.

9. ***Department integration of security and capital planning.***
   The Department of Housing and Urban Development reports a fully integrated capital planning and investment process. Twenty-eight of thirty-nine capital plans reported security costs, and the eleven remaining plans had costs that were covered in other plans. They indicate that all IT investments are clearly linked to the Department's Annual Performance Plan, and the linkages are documented in the IT Investment Portfolio. Integration of IT security with capital planning and investments appears to be the strongest area of the Department's IT security program. The Department indicated that improvements are needed in the estimation of security costs, and not all costs are reflected in their budget request, but plan to adjust the estimates in the FY 2003 budget. The IG found that capital planning has been strengthened in recent years, but cautions that the Department is focusing on monitoring security costs for new systems and a means for monitoring costs of existing systems is still required.

10. ***Critical asset prioritization and protection methodologies.***
    The Department is developing a plan that addresses a number of IT security issues needed to protect assets. It will include frameworks for risk assessments, evaluation of policies, corrective actions, and self-assessments, however the report does not contain any information about the methodology they currently use to identify and prioritize systems and their dependent linkages. The absence of this information, and the IG finding that the Department "has not adopted a methodology to address this area," raises the question of whether the Department understands the point of the question, or fully recognizes the importance of knowing the extent and dependencies of their assets. Without full comprehension of what assets are at risk, and their dependence on other assets within and outside the Department, it will not be possible to protect those assets. Since knowing what needs to be protected is one of the first steps in providing protection, the lack of any methodology to systematically address this issue is a serious weakness in their security program.

11. ***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 submission describes a reasonable set of measures used by the Department to manage the practice of security plans throughout the lifecycle of IT systems. This includes requirements for the development of plans, assigning responsibilities that are reflected in individuals' performance plans, reviewing systems' programs and budget performance, and self-assessments to monitor effectiveness. Although these are all important management processes that are needed to implement an effective security program, this information does not answer the OMB question of what measures of performance are used to ensure the security plans are practiced. Without these measures it is difficult for those responsible for oversight to judge whether or not the plans are actually being followed. Lacking this

information there is no assurance the Department is in compliance with this aspect of the Security Act. This concern is reinforced by the IG finding that the "security program has not evolved yet to the point where security is managed and planned for throughout the IT system lifecycle."

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department has assigned the Critical Infrastructure Assurance Officer responsibility for the integration of IT security with critical infrastructure protection and other security functions. This individual works with area security managers to coordinate activities in support of the IT security program. The Department includes physical, operational, and personnel security as part of the IT systems' reviews and self-assessments. HUD recognizes the complex interdependent nature of their information systems and the need for adequate integration of protections to allow maximum access for legitimate users, while limiting exposure to exploitation.

13. ***Department methods to ensure contractor services are secure.***
    The Department employs audits, reviews, security assessments, and contract provisions to ensure contractor provided services meet the requirements of the Security Act, OMB policy, and NIST guidance. Specific measures of performance were not provided, but the Department reported they are now being documented. The IG found that improvements are still needed in the area of personnel security for critical and sensitive systems.

Department of Interior

1. ***Security funding.***
   The Department of Interior reports planned FY 2002 funding for IT security and critical infrastructure protection of $17.2M. This level of funding comprises 2.7% of their total planned IT portfolio of $628M. The Department has recently redirected an additional $2.3M from other programs.

2. ***Number of programs reviewed.***
   Interior reports reviewing 17 systems identified as critical infrastructures. The reviews represent all systems categorized as either national critical infrastructure (3 systems) or national security (14 systems). The IG reported conducting evaluations of selected IT systems throughout all bureaus.

3. ***Review and independent evaluation methodology.***
   For this first year report, the Department developed its own evaluation methodology to address the seven material weakness areas identified by its IG and GAO. For next year's report, the Department will adopt methodologies recommended by OMB and used in other Departments and agencies. Interior's methodology reviews seven critical areas: policy, plans, accreditation, training, incident handling, contingency plans, and funding. It was also noted that their financial systems' audits include an

evaluation of the security controls. They consider failure in any element to be a reportable weakness with regards to the Security Act. Additionally, the National Security Agency and the GAO conducted selected reviews and audits. The IG also employed their own methodology, which is based on information contained in prior and new audits of the security program, tests of bureaus' evaluations and controls, and review of the Department's policies.

4. ***Material weaknesses.***
The Department has acknowledged its longstanding security weaknesses. Recently, the Department's Management Controls Council reported that IT security was a material weakness, with failures in several specific areas. They include policy standards, certification of IT system plans, testing contingency plans, incident handling, training and funding of IT security throughout an IT system's lifecycle. The breadth of these weaknesses indicate the scope of the challenge Interior now faces in meeting the requirements of the Security Act and raises concerns about how well they are protecting their information resources until they implement broad based security reforms.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
Interior's report does not explain what measures of performance are used to ensure officials have assessed risk, determined security levels, maintained plans and tested controls, nor does it provide any examples of how the Department has performed in these categories. The IG found that "Bureaus did not have adequate IT security practices to ensure that associated operations and assets were safeguarded." The report does describe several general IT security program requirements such as conducting risk assessments, official acknowledgement of risk associated with certified systems, and the maintenance of up-to-date security plans; but it falls short of indicating the measures used to determine success in these areas, or the actual performance. The IG found that bureaus have taken positive steps in developing controls to protect IT assets, but the lack of methodologies to determine correct levels for IT security controls leaves little assurance the controls are appropriate for the systems. The IG also points out that the depth of some system reviews is not always sufficient to determine if controls are effective. The IG expressed reservations about the Department's practice of discontinuing reporting of significant weaknesses when plans were developed, rather than waiting until the corrective action had actually been implemented. The Department reports that it intends to fully exploit the use of all appropriate measures, such as performance evaluations for senior managers and security managers and more detailed and measurable Government Performance and Results Act goals, to motivate and hold accountable its employees and contractors for improved security performance.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The Department's report does not explain what measures of performance are used to ensure the CIO has effectively implemented and maintained security programs, and trained employees. The report contains descriptions of plans for what they intend to do rather than descriptions of actual performance against clearly defined measures. The IG is very direct in their findings when they state that the Department's "CIO does not have an adequate Department-wide security program, has not ensured that the program is implemented, has not evaluated the performance of the program by all bureaus, and has not ensured that agency employees with significant security responsibilities have been trained." The IG report also provides several examples to support this statement. The Department has awarded a contract to develop additional IT security training, including the introduction to IT security seminar, role-based IT security training for executives and senior managers, a training program for systems administrators, security officers, and IT audit personnel, and training for users.

7. ***How the agency ensures employees are sufficiently trained.***

   The Department has established annual training programs, but the resources devoted to training do not appear to be uniform across all bureaus and the reporting was incomplete. The submitted representative sample of staff and training budgets indicate that out of a total work force in excess of 66,000, approximately 16,400 received training. For the employees trained 254 were categorized as systems administrators/specialists, 226 as managers, and the rest as users. For the bureaus that reported, fiscal year 2001 security training costs were approximately $350 for each key system administrator, and averaged between $6 and $125 per employee for security awareness training. Despite specific training requirements in the Computer Security Act of 1987, Interior does not appear to devote adequate resources to training. The IG found that many operating units exhibited weaknesses in IT security awareness and were not able to identify who had received training, or what it cost to provide the training. They also found that most employees and contractors that use IT systems had not received training in their security responsibilities. As mentioned in item 6, above, the Department has already taken steps to address these issues through the development of a comprehensive security-training program.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***

   Interior has established a computer incident response capability that requires verbal reporting of incidents within 24 hours and a written report within 72 hours. Unresolved incidents require a follow-up within 10 days and every 30 days thereafter until resolved. The Department has an agreement with GSA's Federal Computer Incident Response Center to share information and provide recovery services. Incident information is shared between the bureaus via "Information Resource Management Bulletins." However, Interior's report did not describe the Department's actual performance in terms of incidents detected, averted and contained. The IG noted that although some incidents were reported, they found few documented procedures for reporting security incidents and believe further instruction

is needed for reporting incidents. They also found that bureaus are allowed to define what a security incident is, which may effect the consistency of reporting. The IG concludes that the Department needs a formal incident response team to ensure that consistent procedures are followed throughout the Department. The lack of actual incident response performance information in the report, and the IG findings, raises concerns in this area. The Department reports that it has issued a contract to develop a system to correct these deficiencies.

9. ***Department integration of security and capital planning.***
   Interior indicates that the integration of IT security into the capital planning and investment process is a major shortfall area for the entire Department. They have not been effective in tying their IT investments to an IT architecture that fully considers security. The CIO reports they are placing additional senior management emphasis in this area by issuing policy guidance to improve the capture of cost information in capital planning. The IG substantiated this view with their findings that only three of nine bureaus identified costs related to IT security, and only two related the costs to specific systems. Even though capital asset plans indicated that IT security was considered as part of the projects, not all of the capital asset plans included costs for IT security. Without cost information and a consistent understanding of the security requirements it is not possible to integrate IT security into capital asset planning.

10. ***Critical asset prioritization and protection methodologies.***
    In lieu of a Project Matrix review recommended by OMB, Interior uses their own methodology based on guidance found in Presidential Decision Directive 63, "Critical Infrastructure Protection" and a categorization process involving the bureau heads. They report that this methodology gives internal priority to the Indian Trust and other financial systems. Details of how the methodology has been implemented are not given in the report and the determination of dependencies between components and links to external systems is not discussed. The IG found that the three systems identified by the Department as critical assets in its critical infrastructure protection plan, did not have an adequate IT management program to protect them. This does not support the proposition that there is a robust Department-wide methodology for identifying critical assets and their mutual dependencies, without which Interior will not be able to determine adequate levels of protection for its IT systems. To improve this situation the Department is in the process of developing its enterprise architecture and plans to conduct a detailed review of critical assets in FY 2002. The Department has worked closely with OMB in developing its enterprise architecture and in July 2001, accelerated the development with a target date of December 2002. The Department has a detailed plan with eight phases, two of which are scheduled for completion in April 2002.

11. ***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 acknowledges that it has not had adequate measures in place to ensure IT security plans are practiced through the lifecycle of each system. They plan to develop appropriate management tools such as a performance scorecard based

upon NIST guidance. Their report describes high-quality IT security practices used by the Department such as reviews of vulnerabilities, controls and testing, but gives no indication of how the practices are measured or what was the actual performance. The IG found that Interior had issued a draft Department-wide IT security plan and some bureaus update the plans of their more significant systems, however "Information security plans do not exist for every system." Much work remains in this area.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    Interior recognizes the need to integrate IT security with personnel, physical, and operational security, all of which are seen by the Department as separate disciplines. Interior's approach to meeting this objective has been to require the senior managers responsible for the different security disciplines maintain a close working relationship. Since effective integration of different security elements must occur at the system level, and are usually documented in an integrated system security plan, it is difficult to see how the approach reported by the Department will be successful, especially when the report lacks any supporting evidence. The IG's primary observation was that three of the four critical infrastructure systems had some integration of physical and IT security, but disaster plans did not consider IT since the functions would be performed manually (OMB policy states that manual alternatives are not appropriate for continuity of automated processes). As a result of the IG audit the bureau responsible for the systems is in the process of integrating IT security with critical infrastructure protection.

13. ***Department methods to ensure contractor services are secure.***
    Interior reports that it includes standard IT security language into contracts that require IT services. The report does not give any examples of the standard language so it is not known if background investigations, sufficient training, or other measures are required to ensure adequate IT security to protect their systems. There also is no mention of audits, inspections, or other oversight functions the Department might employ to ensure IT security. The IG found that "contracts did not always contain clauses that would ensure adequate security in relation to privacy for web site services." To date, Interior has not established effective Department-wide methods to ensure that contractor provided IT services are adequately secure and in compliance with the Security Act. This issue was a featured agenda item in Interior's recent IT Security Summit.

Department of Justice

1. ***Security funding.***
    The Department of Justice reports planned FY 2002 funding for IT security and critical infrastructure protection of $79.3M. This funding level comprises 3.8% of their total planned IT portfolio of $2.1B.

2. ***Number of programs reviewed.***
Of the 236 classified or sensitive but unclassified cyber security application/program listed in the report, 196 (83%) were reviewed and either approved or conditionally approved within by Department.

3. ***Review and independent evaluation methodology.***
The Department reports using several methods to perform their evaluations, including surveys of their bureaus and asking them to complete questionnaires on selected systems that included many of the reporting elements found in NIST's self-assessment guide and OMB policy. They also relied on documentation submitted for system certifications. In addition, the Department followed OMB, NIST, and industry best practices for their independent verification and validation program and industry best practices for their follow-up penetration test program. The IG reported using several methods to perform their evaluations of five sensitive but unclassified systems and four classified systems. These methods included conducting interviews, on-site observations, and reviews of Department and component documentation. In addition, the IG reported using the NIST self-assessment guide, OMB policy, GAO's Federal Information System Controls Audit Manual and commercial off-the-shelf and proprietary software to conduct security tests and analyses of significant operating system integrity and security concerns. The audits were performed in accordance with Government Auditing Standards.

4. ***Material weaknesses.***
The Department still has significant weaknesses in many aspects of their IT security program. The Department's Report on Management Controls stated that IT security was a material weakness, with failures in several specific areas. The IG reported some of the weaknesses as improper access and password controls, lack of intrusion detection, and inadequate software management including the use of risky programs. The IG found that taken collectively these weaknesses create low-to-moderate risks to the sensitive systems and moderate-to-high risks for the classified systems. While the IG attributes this situation to lack of management commitment for IT security, the CIO disagrees and reports that IT security has been a major priority and a focus of sustained attention throughout the period this report covers. The Department issued an IT Security Order to all of its components, developed a security database to track weaknesses and their resolution, accomplished penetration tests and much of their C&A review activity was conducted throughout the reporting period.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
The percentage of systems accredited is the only measure of performance the Department reported that they use to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls. They show that 83%, 196 out of 236, systems were accredited, which exceeded the goal of 42%. Ninety-eight of 196 systems, 41% of all systems, were granted conditional accreditation that allow operation under specific Department policy which states that conditional accreditations (a) are limited to 180 days and (b) can only be granted when there are

acceptable safeguards and risks and an approved corrective action plan and schedule. Conditional accreditations cannot be granted when system vulnerabilities permit breaches to confidentiality and integrity or impact others. The IG found systems with outdated risk assessments and security plans, and incomplete contingency plans. The Department is recognized for their initial work to use clearly defined metrics to manage their IT security efforts. While the Department and many of its components completed a significant amount of work in certifying and accrediting systems throughout this reporting period, one major bureau failed to perform certification and accreditation for most of their systems.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The report cites three measures of performance used by the agency to ensure that the CIO has implemented an effective IT security program. They are: 1) documented up-to-date policy; 2) ongoing reviews of testing and self-assessments; and 3) tracking of corrective actions. The Department developed a new IT security policy that established baseline security requirements set out in OMB policy and the Security Act, but also established additional requirements to support industry best practices. Some of the highlights of the policy include: formal IT security programs within components; reporting requirements for certification and accreditation, external connections and annual assessments; repercussions for non-compliance; and requirements for IT security to be integrated into the system development life-cycle. The Department's acting CIO reports taking action against components for non-compliance with the Department's program. These actions have included withholding funding for new initiatives until an acceptable corrective action plan has been established and shutting down component systems until safeguards have been implemented. No other agency reported taking such specific and significant action. The Department does admit to a number of weaknesses revealed in accreditation reviews that are now being worked. The IG found seven systems with security plans that were incomplete, unimplemented, or not enforced. One system had no policy, procedures or plans, and one system only had them in draft form.

7. ***How the agency ensures employees are sufficiently trained.***

   The Department has established annual training programs, but does not identify the relationship between the types of training being given and the requirements for a sufficiently trained staff. This makes it difficult to assess the adequacy of the Department's IT security training. The Department reports that $1.7M of their $60M FY 2000 security-budget was spent on security training and shows that over 126,000 employee training sessions were given for the Department's 121,000 employee. Training resources varied greatly by bureau, from about $0.50 to $80 per employee. This variance can indicate a number of things ranging from more sensitive activities requiring more training to questions concerning whether the Department is effectively managing training resources across all bureaus. Because of the way the data is presented in the report it is not possible to determine if the funds spent on different types of training is consistent with the norms established by other department and

agency reports. The Department appears to be making a substantial effort to adequately train their employees, uses classroom and video instruction, distribution of handouts, and emails to computer users for security awareness training. However, the weaknesses in maintaining training records reported by the IG and the mixed presentation of the data provided in the report, make it difficult to determine if department-wide the work force is being adequately trained.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department and the IG that Justice has a department-wide incident response and information sharing capability that operates around the clock supporting all bureaus. Additional services provided by Justice's Computer Emergency Response Team are security alerts, inquiry response, and web page Intranet information sharing. The Department notifies GSA's Federal Computer Incident Response Center and the FBI's National Infrastructure Protection Center of incidents involving external resources. The Department provided data showing 52 incidents reported for the year ending June 2001. The Department has a well functioning incident response capability. It is difficult to assess performance without additional information on actual performance beyond knowing the number of total attacks.

9. ***Department integration of security and capital planning.***
The Department integrates IT security into their capital planning process with an IT Investment Management policy that provides a framework for managing IT portfolios. This policy requires its bureaus to address IT security issues in an investment's selection phase, identify requirements in the control phase, and periodically reassess IT security as part of the operations phase. This is a reasonable and valid approach, but the Department did not answer the question of whether security requirements and costs were reported on every FY 2002 capital asset plan submitted to OMB, and if not, why not. The IG offered no comments in response to this topic. At the same time, as reported in item six, above, the Department has withheld funding for new IT initiatives until an acceptable corrective action plan has been established and has shut down component systems until safeguards have been implemented. This is certainly indicative of effective activity in this area.

10. ***Critical asset prioritization and protection methodologies.***
Although the Department has elected not to use Project Matrix as suggested by OMB, the methodology described in their report contains its most important elements and appears to be a valid approach for the identification and prioritization of critical assets. Their methodology uses several sources of information to generate an inventory of critical systems, is augmented by information in Justice's strategic plan, guidance from Presidential Decision Directive-63, and consultations with Commerce's Critical Infrastructure Assurance Office. The process also includes techniques for linking the systems to the Department's goals and dependencies to other systems, in a matrix that includes physical and operational assets. They report that they now have a list of critical IT, personnel, and physical assets that include asset name, location, description, and strategic goal supported, potential impact of loss, and interdependencies. While this approach is effective for one Department,

Project Matrix compiles the data from all agencies to support gap analysis across the government's enterprise. OMB will discuss this with the Department of Justice.

11. ***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 initial report from the Department did not contain any examples of measures of performance used by the agency to ensure practice of IT security plans throughout the lifecycle of each system, or actual performance assessed against the measures, as requested by OMB. In subsequent discussions, the Department provided additional information to OMB on efforts begun during the reporting period to ensure compliance with security policy and with the implementation of IT security plans throughout the system life cycle. These efforts include the work of the Department's Compliance Review Group, operated by the Department's Security Officer. During FY 2001, the review group visited 55 departmental sites throughout the country. In addition, the review group completed three reviews of specific component IT systems. Additionally, the Department reviewed over 100 system certifications and accreditations completed by component program managers, and conducted independent verification and validation on 12 systems. The Department completed nine penetration tests of component systems and reviewed the results of NSA penetration testing activities on two more. The weaknesses identified through these efforts are tracked in the Department's database until corrective actions are completed. In addition, selected follow-up reviews are performed of completed corrective actions. The IG only noted that of the nine systems audited, five had a lifecycle management process within their security plans, and four had not implemented a lifecycle management process.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department relies on incorporating Presidential Decision Directive-63 requirements into their IT systems Certification and Accreditation guide as a primary means of integrating IT security with critical infrastructure protection, physical, personnel, and operational security. As the bureaus certify their systems they document the requirements needed to integrate the various security elements. The Department also reports that they conduct certification testing in all of the security areas to determine if controls are in place. The IG did not provide comments or findings for this area.

13. ***Department methods to ensure contractor services are secure.***
    The Department and the IG report that while contractors have access to sensitive data, 44% of them did not have the necessary background investigations. The Department has issued new guidance for hiring contractors and directed the bureaus to establish a timetable to quickly correct this problem. New contracts must include a clause to identify the Department's requirements, and current contracts will be amended as they are modified or renewed. The report does not refer to any other specific methods (e.g. contract language, regular audits or inspections) to ensure contractor provided IT services are adequately secure.

Department of Labor

1. ***Security funding.***
   The Department reports planned FY 2002 funding for IT security and critical infrastructure protection at $67M, almost a five-fold increase over FY 2001. This level of funding comprises 17% of their total planned FY 2002 IT portfolio of $393M. The reported percentage for security is significantly higher than that reported by any other department or agency.

2. ***Number of programs reviewed.***
   Of the 52 major applications and general support systems as defined by OMB policy and critical infrastructure systems relevant to Presidential Decision Directive 63, "Critical Infrastructure Protection," distributed throughout the Departments 13 agencies (bureaus), all are reported as having been reviewed. The IG found that out of the 10 major application/systems they evaluated, four had not been reviewed in the last 3 years.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide as their review methodology. This methodology is derived from the Federal CIO Council's Information Technology Assessment Framework and is recognized throughout the government as an effective analysis tool. Department-wide adoption of this practice is the right approach, however the IG finds that it is not yet a uniform practice.

4. ***Material weaknesses.***
   The Department reported that they are in substantial compliance with all Federal laws and did not identify any "systemic or structural weaknesses." The Department recognized that material weaknesses had been found by the IG, but indicated that remediation plans will be submitted. The IG found that although the Department has detailed security policies and procedures guidance, they were only partially implemented in the ten major applications evaluated and not practiced in one of six support systems evaluated. The IG discovered weaknesses in virtually every area of IT security including access controls, certification, and incident reporting. The most serious finding was the IG's ability to penetrate a number of systems they tested. The IG noted that the bureaus acted quickly to correct deficiencies detected by the IG, but their inability to detect these problems until an IG investigation (as well as their persistence over a number of years) raises concerns about the effectiveness of the Department's security program implementation.

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   The report describes measures of performance for three tasks: system risk assessments, security plans, and controls testing and that 51 of 52 major applications/programs have completed risk assessments and security plans. No data was provided on how many systems' security controls were tested. The CIO report also indicates that the agency has measures in place to ensure officials have assessed

risk, and are maintaining plans, but it does not indicate whether they have determined security levels and tested controls. The IG reports indicates that implementation is inconsistent, e.g., bureaus have "performed some risk assessments" and "have security plans that indicate that some level of security assurance functions are being carried out." The IG also reports that for ten bureau-level applications, "specific measures of performance have not been developed" and "formal performance measures do not exist for program officials."

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The report explains how the Department mandates the requirement for security plans and grades the CIO on the number of risk assessments and security plans that have been accepted. However, the report does not identify whether measures are used to evaluate the implementation and maintenance of the security program. Both the IG and supporting documentation indicates that at the bureau level, milestones are being tracked and the bureaus have substantially complied with security planning requirements. However the IG finds that bureaus "do not have a fully implemented security program." The IG also reports that they "could not identify any specific measures of performance at the [bureau] level to ensure that an acceptable level of performance has been attained."

7. ***How the agency ensures employees are sufficiently trained.***
   The Department has established annual training programs, but the resources devoted to training are not uniform across all bureaus and the reporting was incomplete. The Department reports that at least $258,000 of the $14.5M FY 2001 security budget was spent on training. The information describing training attendance and costs indicate that 4,074 employees were trained out of a total work force in excess of 16,420 (25%), of which 54 were categorized as having significant security responsibilities (0.3%). The Department does not report how many of their employees required basic awareness or specialized training. For the bureaus that reported, FY 2001 security awareness costs are estimated to be $50 for each employee trained and $1000 per person for specialized training. The IG found that "overall the department did not have a structured IT security-training plan to ensure that its employees are sufficiently trained in their security responsibilities." The IG goes on to say that the Department lacks a minimum plan that defines core training standards, documented requirements, and costs. The IG also noted that one bureau had developed its own guidance and procedures for security awareness training.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   The Department does not have a fully effective incident response capability. Some progress has been made in the last year and the Department's Computer Security Handbook defines the procedures for reporting incidents, but the IG found there is "minimal evidence of incident reporting capabilities" and numerous deficiencies exist for the detection and sharing of incident information. While the Department reports that within the Office of the CIO an incident response team maintains constant

contact with national incident response coordinators such as GSA's Federal Computer Incident Response Center and the FBI's National Infrastructure Protection Center, the IG found a need to establish an "official" incident response team. OMB policy requires all agencies to have such a capability.

The Department reports that over the past 18 months, 23 incidents required a response and while four of them involved unauthorized access, only one was judged to warrant external reporting. The low number of total incidents reported raises questions as to whether the Department has an effective detection program. The IG reports that the Department needs to establish efficient logging/tracking mechanisms. Weaknesses in detection and reporting may be a factor in low numbers of reported incidents. While it appears that the Department may not be complaint with the Security Act's requirements in this area, their report does not acknowledge any shortcomings or indicate planned improvements.

9. ***Department integration of security and capital planning.***
   The Department manages the integration of IT security into their capital planning investment process by including security considerations in their Systems Development Lifecycle Process. This includes screening and scoring questions and post implementation reviews. While the Department did not address in their report whether security requirements and costs were included in every capital asset plan and included in their budget submission, OMB and the Department have resolved this issue and all submissions are complete. This reconciliation post-dates, the IG's finding that the budget submissions for three bureaus "did not show any specific detailed security requirements and costs." The Department has one of the better processes in place for integrating security and capital planning and is continuing to improve it.

10. ***Critical asset prioritization and protection methodologies.***
    Due in part to earlier IG concerns, the Department has now undergone the first phase of a Project Matrix review to identify, prioritize and determine the interdependencies of their critical assets. Later phases will begin this year. OMB has directed all large agencies to take this approach. The Department has also sought guidance from the Critical Infrastructure Assurance Office to assist developing a Department Critical Infrastructure Protection Plan.

11. ***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 report does not include any examples of measures of performance used to ensure practice of IT security plans throughout the lifecycle of each system or the actual performance assessed against the measures. The Department only provided information about guidance concerning the system development lifecycle. The IG found that for the ten applications evaluated, no bureaus had developed specific measures of performance to ensure the practice of IT security plans. The report's lack of attention to this important topic raises concerns as to management efforts to ensure that security plans are being implemented throughout the Department. The IG also

found that without the existence and practice of performance measures, the Department could not be assured that IT security is being managed throughout system lifecycles.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The report indicates that the Department assigned the CIO responsibility to oversee both IT and Critical Infrastructure security. The CIO is also to ensure integration of these elements at all levels and aspects of the plans and programs. This includes each system's compliance with the Department's contingency planning requirements. The IG found that the bureaus submit security plans to the CIO for review, but plans are not fully integrated with other forms of security. The IG reports that critical infrastructure protection plans are not associated with the physical security plans for the facilities that house the critical systems and that physical protection plans for minimum essential infrastructure was outdated. The IG found that the Department is taking steps to make improvements in this area.

13. ***Department methods to ensure contractor services are secure.***
    The Department relies primarily on background screening, contract language, and the terms/conditions of the contract to ensure the security of contractor provided services. The IG found that the Department does not conduct any additional inspections or audits, but did conduct a mitigation conference to resolve specific contractor security issues.

National Aeronautics and Space Administration

1. ***Security funding.***
   The National Aeronautics and Space Administration reports planned FY 2002 funding for IT security and critical infrastructure protection of $105M. This funding level comprises 4.1% of their total planned IT portfolio of $2.55B.

2. ***Number of programs reviewed.***
   NASA reports reviewing cyber-security programs at all five of its enterprises and eleven field centers including headquarters. The Security Act and OMB reporting guidance required a review of all agency programs and systems. The IG reported evaluating more than 130 systems located at ten field centers and headquarters.

3. ***Review and independent evaluation methodology.***
   The Agency chose to develop their own assessment methodology rather than use the ones suggested by OMB. The Agency's methodology consists of guidance, goal setting, monitoring activities, developing and implementing plans, and performance measures, and is augmented by external evaluations. The National Security Agency concluded that the Agency's IT security program was maturing, with two areas needing improvement: the decentralized management structure of the program and the need to expand existing policies to account for changes and new technologies.

NASA did not provide information on the methodology used to support this assessment including whether it comports with the Security Act, OMB policy, or NIST guidance.

4. ***Material weaknesses.***
   Although NASA acknowledges several areas of significant management concern, the Administrator determined that none were considered material weaknesses. The IG reported significant improvement in the Agency's IT security program, but still found numerous weaknesses that had yet to be addressed, many of which had low-cost or no-cost solutions. The IG "continues to identify weaknesses in the controls for implementing the Agency's IT security program," specifically in IT security training, and planning and implementing IT security. They repeatedly found that the CIO fails to communicate IG findings to the community within the Agency, which hampers NASA management efforts to minimize vulnerabilities and track improvements. The most serious weaknesses identified by the IG were the lack of training for individuals with significant IT security responsibilities, no consistent Agency security program, and the lack of enforcement mechanisms to ensure implementation of security policies. While the Agency's IT security practices are more mature than many other agencies, the IG believes that management is unwilling to recognize the significance of the weaknesses and deal with them in a timely manner. The IG "considers IT Security to be a material internal control weakness reportable in accordance with the Federal Managers' Financial Integrity Act."

5. ***Measures of performance used by the agency to ensure officials have assessed risk, determined security levels, maintained plans, and tested controls.***
   NASA has established measures of performance that place responsibility for IT security in the hands of the program/project managers, with the CIO providing guidance. They report that security plans are in place for 97% of their special management attention systems and intend to address the remaining lower priority systems by July 2002. This is a good step, but OMB notes that security plans have been required for all agency systems for many years. The IG found that some of the plans "lacked significant required elements." Coupled with shortcomings in the critical IT asset inventory, the IG believes that the Agency cannot provide sufficient evidence that all necessary plans are in place or that they comply with requirements of the Security Act and OMB policy. Penetration and vulnerability testing of applications and systems is conducted on an ongoing basis and is among the most comprehensive reported by any agency. However, the IG believes that insufficient time is allotted for assessing vulnerabilities on the Agency's complex networks. Policies and rules directing officials to give IT security a high priority are in place, but it is not clear how performance will be assessed or the policies enforced.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   NASA's CIO is assigned responsibility for identifying and reporting threats, documenting plans, training employees, and reviewing systems for compliance with

Agency directives. To measure compliance, directives contain metrics such as the number of plans in place, employees trained, and the number of IT security incidents. The IG found that although measures of performance exist, they are not adequate to ensure an effective security program. For example, the IG notes that none of the 2,817 contractor systems administrators, who comprise 79% of all NASA's systems administrators, are included in the training performance measure. The Agency should ensure adequate training for all personnel as required by the Security Act and OMB Policy. The Agency should also develop accurate performance measures to accurately assess all program requirements including training. OMB does find it healthy however that the Agency has developed measures that are worthy of substantive discussion. Many agencies have not progressed this far.

7. ***How the Agency ensures employees are sufficiently trained.***
NASA has established annual training programs and is making effective use of web-based technologies to provide IT security training. The Agency reports that over 90% of their 54,246 Federal and contractor employees received general awareness training within FY 2001. However, the IG reported that training for 2,817 contractor systems administrators out of a total of 3,588 total systems administrators was not considered as one of the security program's performance measures. As discussed in item six, above, ensuring the security of an agency's operations and assets demands that all employees (Federal and contractor) be adequately trained and measuring the performance of such a program requires measuring all elements of it. The IG also reported that only 50% of the Federal employee system administrators with significant IT security responsibility had received training at the time of their review.

The Agency did not provide IT-security training costs and the IG found that the Agency's decentralized approach to training "contributes to funding and staffing shortfalls." However, the Agency reports the use of a centralized web-based training system to deliver primary training to users, system administrators, and managers. Records are kept of the training delivered and the score received. The IG also "determined that the Agency was not moving aggressively to ensure that all individuals were appropriately trained," and that lack of sufficient IT skills puts the Agency at risk of compromising its IT resources. OMB looks forward to improved program performance and measures to evaluate all aspects of the Agency's training responsibilities.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
NASA established an agency-wide Incident Response Center in 1993 to deal with attacks and communicate with external organizations such as GSA's Federal Computer Incident Response Center. In FY 2000, their Incident Response Center distributed over 1,400 security alerts. The IG findings noted that the Incident Response Center was not following IG recommendations to strengthen NASA's incident response capability to be more active in planning penetration tests, evaluating solutions, and training materials. They also found that the Agency has still not addressed their 1999 recommendation to standardize incident reporting and effect strong management controls.

9. ***Agency integration of security and capital planning.***
NASA reports having generally integrated security into its IT capital planning control processes but indicated further improvement is needed. The IG indicated that the Agency did not include security requirement and cost in its capital asset plans, and does not plan to submit all plans for FY 2002 as requested by OMB. The IG further found that the Agency had not calculated IT security costs on a system-by-system basis as required by OMB budget guidance, but plans to do so in the future. Since the Agency did not separately report security requirements in their FY 2002 budget materials, the IG could not determine the extent to which IT security is integrated into the capital planning process. However, NASA has reported security costs on their FY 2003 budget materials.

10. ***Critical asset prioritization and protection methodologies.***
NASA uses its own methodology in lieu of a Project Matrix review. They report that this methodology focuses on identifying system components containing information or performing functions that justify special management attention. While this approach is effective for one Agency, Project Matrix compiles the data from all agencies to support gap analysis across the government's enterprise. OMB will discuss this with the Agency. Under the NASA methodology, the components are categorized according to risk and assessments are made that provide a basis for the security plans. Identifying interdependencies between components and links to external systems is not discussed. OMB finds this to be an essential component of such an exercise and a key feature of Project Matrix. The IG found that this methodology did not accurately identify all minimum essential infrastructure (MEI) assets (specifically, National Resources Protection assets that NASA defines as crucial to the success of NASA missions) and therefore the Agency may not be adequately protecting its critical assets. Agency management disagrees with the IG finding. If an asset is crucial to mission success, then its absence from such an inventory is troubling. The IG also reports that it has been over one year since the Agency said it would implement procedures for updating the MEI list. NASA has since issued guidance, but the list has not yet been updated. The IG found that the Agency cannot adequately prioritize the criticality of its IT assets, or adequately identify the interdependencies essential to the physical infrastructure, and as such is unable to appropriately protect them.

11. ***Measures of performance used by the head of the agency to ensure the security plan is practiced throughout the life cycle of each system.***
NASA reports that plans are in place for 97% of their systems requiring special management attention and 72% of the remaining systems are also covered. These plans contain instructions for implementing security procedures and measures of performance to determine their effectiveness. Although the Agency requires security plans for each field center and system, the IG found that the "CIO did not develop a performance measure to ensure that the Agency's IT security plan is practiced." Law and policy have required security planning for many years. It is important for the Agency to quickly complete and implement such plans for all Agency systems.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Agency reports that its critical infrastructure protection program is integrated with its IT security program. The Agency's program operating plans contain measures of performance that address specific areas of concern. The IG reports that although the plans have generally been developed, the IG will not have an opportunity to review their implementation until FY 2002. Effective integration of all aspects of security is vital to understanding threats and security needs.

13. ***Agency methods to ensure contractor services are secure.***
    The Agency reports that their procurement regulations require contractors to comply with the same standards that apply to its Federal employees. These clauses apply to all IT systems operated by the Agency. External consultants are routinely used to conduct assessments and audits of contractor compliance with IT security guidelines. Audits and inspections by the IG are also used to verify contractor adherence to security requirements. The Agency's standard procurement clause for IT security includes detailed requirements for background investigations. The IG found that although the requirement of contact security clauses have been in effect for about 6 months through June 2001, one of the three field centers reviewed had not identified all the contracts subject to the clauses. The IG goes on to state that the Agency does not include applicable IT security requirements in purchase orders (contracts), grants, and cooperative agreements.

National Science Foundation

1. ***Security funding.***
   The National Science Foundation reports planned FY 2002 funding IT security and critical infrastructure protection of $1.56M. This level of funding comprises 5.2% of their total planned FY 2002 IT portfolio of $30M.

2. ***Number of programs reviewed.***
   NSF reported that their review focused primarily on the Agency level security program managed by the CIO, augmented by selected reviews of critical systems within other NSF organizations. NSF was one of the few departments or agencies that chose to define "program" at such a high level. The Security Act and OMB reporting guidance required the review of all programs and systems. While NSF is a small agency (about 1,300 employees) and an agency-level program review may be appropriate, it should include a review of all systems comprising its IT portfolio.

3. ***Review and independent evaluation methodology.***
   NSF used the NIST self-assessment guide to evaluate their security program, supplemented by CIO generated self-assessment surveys for each organization. The majority of responses to the survey questions were based on evaluations of the overall agency security program, with a subset of the questions focused on "mission critical"

system assessments. The NSF Security Officer has reviewed the results to provide a preliminary assessment. A more in-depth analysis is underway. The IG used GAO's Federal Information System Controls Audit Manual supplemented by the NIST guide as their methodology.

4. ***Material weaknesses.***
   The Agency did not report any material IT security weaknesses. The IG indicated they had identified areas where improvements were needed in the Agency's computer security, but did not judge them to rise to the level of material weaknesses. Although no material weaknesses is normally a good sign, the lack of supporting documentation and possible indications of weaknesses in Agency's IT security practices elsewhere in the Executive Summary are cause for concern. The Agency does not provide enough information to validate their assessment that IT security deficiencies are not reportable as material weaknesses. For example, their reported actual performance for "penetration testing of IT controls" was "yes" rather than a percentage, and no information was provided on training requirements, cost, and attendance.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency reported that for mission critical systems, 80% of the risk assessments and 95% of the security plans had been completed, however the IG noted that only 40% of these plans had been approved. The response for the goal of "Independent reviews and annual penetration testing of IT controls and assets" was "yes", which could mean anywhere from 7% to 100% of the mission critical systems were tested. The agency did not indicate any measures of performance used by the Director to ensure officials had determined security levels. The IG found these measures of performance "were appropriate for the first year of the [Security Act] implementation," however this statement overlooks that the head of the agency has been required by statute to ensure adequate IT security for many years. OMB's guidance stated explicitly that Government Performance and Results Act-like performance measures were not being sought. The IG observed that they expect future measures of performance will be developed to validate self-assessments, system certifications, and security training.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   NSF offered few specific measures of performance used by the Director to ensure that the CIO effectively performed their responsibilities. Specifically, for critical systems they had completed 80% of the risk assessments, 95% of the security plans (40% approved), had performed some penetration testing, and had some IT security policies. They also report that 87% of staff with significant IT security responsibilities has completed training. The information provided is not adequate for OMB or the agency head to assess whether the CIO is implementing and maintaining an effective IT security program.

7. ***How the agency ensures employees are sufficiently trained.***
   The agency has established annual training programs and is making constructive use of web-based technologies to provide IT security training, which is available to all of their 1,320 employees. The report provides a reasonable description of the IT security training offered by the Agency, but does not indicate how many employees should be receiving the various types of training, nor did the Agency comply with the OMB guidance to report IT-security training costs. The Agency reported 87% of the staff with significant IT security responsibilities completed training. The IG found that the Agency "needs to develop and implement procedures for tracking the number of employees that receive each type of security training, capturing the costs of its security training program, and ensuring that all employees receive periodic security training." Without knowing how many people were trained, what it cost to train them, and how many should have been trained, the agency cannot know whether adequate resources are being devoted to training.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
   The agency has established an agency-wide Incident Response Team to deal with attacks and share information with external entities like the GSA's Federal Computer Incident Response Center. The Agency's report provides some examples of how agency personnel and the Incident Response Team should handle IT security incidents and reporting. These procedures were documented in 2000 and included in a formal agreement between the CIO and the IG. The Agency indicated that three incidents were reported last year, but did not respond to the OMB's request for actual performance regarding identifying vulnerabilities, detecting and deflecting attacks, dealing with incidents, and sharing this information with other organizations.

9. ***Agency integration of security and capital planning.***
   NSF reports their planning document states that IT Security requirements and costs must be addressed as part of their capital planning and investment control process. The IG noted that the guidance is undergoing review to ensure security considerations are explicitly documented and periodically reviewed. Although the Agency considers IT security internally for their planned initiatives, the IG found that the Agency does not separately delineate IT security in their report to OMB, but does include the costs in the overall budget request.

10. ***Critical asset prioritization and protection methodologies.***
    The Agency did not specify or describe the methodology they are using to identify, prioritize, and determine the interdependencies of their critical assets. The IG reports that the CIO requested that the organizations complete surveys, which resulted in the identification of 15 mission critical systems within the Agency. However, there is no indication that the assets were prioritized or the interdependencies between assets within and outside the Agency were determined.

11. ***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 measures of performance used by the Director to ensure the security plan is practiced throughout a system's lifecycle were the same three performance measures listed in response to item five, above. They reported that for mission critical systems, 80% of the risk assessments and 95% of the security plans had been completed, of which 40% had been approved. The response for the goal of "Independent reviews and annual penetration testing of IT controls and assets" was "yes", which could mean anywhere from 7% to 100% of the mission critical systems were tested.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Agency indicated that it has no critical infrastructure as defined by Presidential Decision Directive-63, but has integrated its IT security program with other security elements by having the Automated Data Processing Security Officer work closely with the Division of Administrative Services, which has responsibility for physical security.

13. ***Agency methods to ensure contractor services are secure.***
    The Agency reports that it complies with Security Act and OMB guidance by including standard IT security language into contracts that require IT services conform to Federal security guidelines and mandates. The report does not give any examples of the standard language so OMB does not know if background investigations, sufficient training, or other measures are required to ensure adequate IT security to protect their systems. The report does mention that the Agency relies on annual IG audits of financial systems for protection of their IT infrastructure, and has recently contracted for an intrusion detection service.

Nuclear Regulatory Commission

1. ***Security funding.***
    The Nuclear Regulatory Commission reports planned FY 2002 funding for IT security and critical infrastructure protection of $1.4M. This level of funding comprises 2.2% of their total planned IT portfolio of $64M.

2. ***Number of programs reviewed.***
    The Commission reported reviewing one cyber-security program that covers the entire agency. The review included self-assessments of 21 major applications and one general support system, but does not indicate how many total applications and support systems the agency has. The IG reported evaluating the Agency's overall IT security program, the self-assessments of the 22 major application/systems, and the security controls for five representative systems.

3. ***Review and independent evaluation methodology.***
   The Commission used the NIST self-assessment guide to review their information technology systems. In addition to the NIST guidance, they developed a supplemental survey to capture information needed to comply with Security Act reporting requirements. The IG engaged an independent contractor to review the Agency's IT security program and prepare an annual independent evaluation as required by the Security Act. The IG's contractor used their own methodology that included a background review of the security program, evaluation of the plan, and the Agency's compliance with the Security Act using the NIST standards for guidance.

4. ***Material weaknesses.***
   The Agency acknowledges several areas of concern that merit management attention and requires corrective action, but the IG points out "Determination of material weakness, if any, was based on detecting mission critical deficiencies. No mission critical material weaknesses were found that warranted identification and reporting under other law." The IG also reported the Agency's security program is comprised of a comprehensive set of policies, but its implementation is incomplete. They found that the lack of central oversight and measures of performance result in a weakened security posture and risk of loss, misuse, unauthorized access to, or modification of information.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency indicates that it has not established measures of performance for, nor does it discuss in their report, how they ensure officials assess risk, determine security levels, maintain plans and test controls. The report acknowledges that the security program is "lacking in management oversight" and "There is neither an oversight role nor any system of accountability for IT security within the [agency]." The report goes on to state that not all systems have security plans, which are generally the system owner's responsibility, and "These individual plans have not been integrated into a centralized security plan or methodology." The lack of planning is troublesome inasmuch as law and policy have required it since the enactment of the Computer Security Act of 1987. The report quotes a recent GAO finding that identified IT security as a major challenge for the agency, and that it "has no goal, strategy, or measure to address the challenge on an agency-wide basis."

   The IG reported that risk assessments are not being performed for all systems, nor does the agency have any measures of performance to determine if the level of security identified for a system is appropriate. Here it is important to note that neither OMB policy nor the Security Act require formal risk analyses for agency systems, but they both require that all systems be adequately secure based upon an understanding of risk and magnitude of harm. For the overall reporting period, the agency was not in compliance with Security Act requirements in this area, but it reports it had already begun an aggressive correction program prior to the end of the reporting.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***

   The Commission reported that the status of individual systems' security environments, and hence the total IT security program, is not routinely known because there is no Agency-wide oversight or compliance monitoring. There are also no performance measures in place to capture relevant performance data regarding IT security. The Agency-wide security program guidance prepared by Office of the CIO leaves responsibility for implementation and monitoring IT security policy to the system owners rather than a central authority, due to agency funding priorities. While centralized implementation is not a good approach, centralized monitoring is important. The IG finds no evidence of an agency-wide security plan nor has the Agency appointed a senior information security official that reports to the CIO, as required by the Security Act. The IG also reported that there was no way to track training compliance to ensure employees and contractors are sufficiently trained.

7. ***How the agency ensures employees are sufficiently trained.***

   The NRC conducts periodic training programs and is making constructive use of web-based technologies to provide IT security awareness training, but due to lack of recording keeping they are unable to report how many of their 2,800 employees actually received general awareness training. The report also neglects to mention any advanced training for system administrators, which is needed to ensure their skills are up-to-date. The Commission did not comply with the OMB guidance to report IT-security training costs, but the IG noted that there is an annual training budget of $1,500 to $2,000, which averages less than $1 per employee. The IG generally found that despite specific training requirements in the Computer Security Act of 1987, the Commission couldn't show that it devotes adequate resources to training. Although annual IT security awareness training and new employee indoctrination is mandated by the agency, it does not specify training requirements for system administrators and employees with significant IT security responsibility, or track who received training. The IG further found that there is no mechanism to ensure employees receive required training. The Commission asserts, however, that the deficiency in this area is one of inadequate monitoring, not poor training practices, and has begun addressing the monitoring deficiency. This is a step in the right direction since without monitoring one cannot understand or validate program performance.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***

   The NRC has not established a consistent agency-wide formal incident reporting process, but has documented procedures for logging and forwarding incident event information. The agency also monitors external entities like GSA's Federal Computer Incident Response Center and NASA's Incident Response Center to receive warnings that are then distributed throughout the agency. The IG noted approximately 30 unusual behavior incidents (scans), and 30 attacks are logged each month and reported internally. Incident reporting to the IG is at the discretion of the system owner. The agency is not aware of any successful attacks in the last three years, and therefore has not reported any incidents outside of the agency. The IG expressed

concern that the only intrusion detection methods described by the agency were in reference to attempts via the firewall and do not address any other kinds of intrusions or detection methods. Weakness in incident detection and reporting make it difficult to know when an incident has occurred, and may be a factor in the low number of incidents reported.

9. ***Agency integration of security and capital planning.***
   The agency reports that IT security requirements and costs are integrated into its IT capital planning and investment control processes and are included in the FY 2002 capital asset plans included in their budget submission to OMB. The IG expressed concern over the agency practice of rolling up the security costs into other programs. If changes occur to the funding category where security is included, the security funding could be lost or re-appropriated. OMB is working with all agencies to improve their reporting in this area.

10. ***Critical asset prioritization and protection methodologies.***
    The NRC uses its own methodology in lieu of a Project Matrix review. This methodology focuses on identifying system criticality and protection requirements. Criteria are given to determine if systems are mission critical, general support, or business essential systems. The agency also adopts the NIST sensitivity/criticality assessment methodology to rate the confidentiality, integrity, and availability of systems. Identifying and addressing system interdependencies between components and links to external systems is not discussed. Identifying interdependencies and the unintended consequences of such is a key feature of a Project Matrix review and is among the reasons that OMB has directed all large agencies to undergo such a review. The IG found that the policies and procedures for protecting critical assets are adequate, but the implementation is inconsistent, and the lack of centralized oversight and enforcement over policies renders them ineffective.

11. ***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 reports, and the IG concurs, that the Agency does not have measures of performance to ensure that IT security plans are practiced throughout the lifecycle of their systems. As a result the agency has limited assurance that specific IT risks are considered or controls implemented for all IT systems.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Agency provided information documenting the integration of security programs.

13. ***Agency methods to ensure contractor services are secure.***
    The Agency reports that the National Institutes of Health is the only external provider of IT services. The last audit of NIH was performed over one year ago and revealed no "material security-related discrepancies." Despite the requirements of the Security Act and OMB guidance, the Commission did not evaluate the security of NIH provided services for the purposes of this report. Until such an evaluation is

performed and adequate security performance is validated, the Commission is not compliant with the Security Act in this area. An important feature of such an evaluation should be to identify NIH interconnections.

Office of Personnel Management

1. ***Security funding.***
   The Office or Personnel Management reports planned FY 2002 funding for IT security and critical infrastructure protection of $4.3M. This funding level comprises 4.7% of their total planned IT portfolio of $92M.

2. ***Number of programs reviewed.***
   OPM did not report their full inventory of major applications and general support systems, and indicated that only seven systems were evaluated for this report. The Security Act and OMB reporting guidance called for a review of all programs and systems. The IG focused their efforts on assessing the implementation of the agency-wide security program and examine access controls for the Agency's mainframe computer.

3. ***Review and independent evaluation methodology.***
   The Agency used the NIST self-assessment guide to review seven of their information technology major applications and systems. The IG used OMB policies and guidance supplemented by interviews of program officials and individuals with significant security responsibilities, reviews of existing documentation provided by the OPM staff, a financial statement audit conducted by a contractor, and NIST guidance.

4. ***Material weaknesses.***
   The IG reported that they had identified areas they classified as "reportable conditions," but they did not judge the deficiencies to qualify as material weaknesses, and neither they nor the Agency reported any material IT security weaknesses. The IG cites a number of underlying causes for the weaknesses in IT security including no Agency-wide security program or formal methodology for risk assessment, incident handling, integration of capital planning, and fails to comply with security training responsibilities.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency reports that it issued an agency-wide IT security policy, but is still in the process of implementation. The report does not provide measures of performance or examples of actual performances used to ensure program officials are fulfilling their responsibilities. The Agency did not describe how they will motivate program officials to ensure they have effective IT security programs or how the policies will be enforced. The IG reports the Agency does not have a formal methodology for

assessing risk, but they do maintain a security plan for mainframe operations, and have implemented procedures for system activity audit trails and reporting violations.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Agency report does not explain the measures of performance used to ensure the CIO has fulfilled their responsibilities, other than to state that she has been assigned this role and responsibility. They report that they are in the process of implementing IT security policies, which will develop the necessary measures of performance. The IG found that the Agency has not implemented an agency-wide security plan, and although some of the required elements are documented, there is no integrated IT security plan.

7. ***How the agency ensures employees are sufficiently trained.***
   The Agency reports that it has established annual training programs and has provided IT security awareness training to almost 100% of their 2,800 employees at an estimated cost of $40,000 (approximately $15 per employee). They also report that attendance records are kept. For specialized training required for employees with significant IT security responsibilities, the Agency did not indicate the number or type of training, only the estimated cost of $4,000. The IG found that "The CIO has not implemented a security training program to ensure that employees with critical IT security responsibilities are sufficiently trained to carry out these assignments, as required by the Security Act."

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
   The Agency does not have a fully effective incident response capability, although some progress has been made in the last year drafting procedures for appropriate notification to GSA's Federal Computer Incident Response Center and the FBI's National Infrastructure Protection Center. The IG found that although elements are in place, the Agency does not have a formally established computer incident response team, and is not in compliance with OMB policy which requires Federal agencies to have a IT security incident response capability. They concluded that the Agency's lack of capability in this area could cause existing or potential vulnerabilities to escape detection. The Agency only reported one incident last year.

9. ***Agency integration of security and capital planning.***
   The Agency reports that it currently uses a "less formalized" process to integrate information security into its capital planning and investment control process. They focus their attention on their two major systems and state that estimated security costs were reported on their capital asset plans in their FY 2002 budget submission to OMB. The IG found that "[the Agency] does not adequately integrate security requirements or cost estimates into its capital planning and investment control process as required by OMB budget guidance. The IG noted that while the two capital plans submitted discussed IT security, the written justifications did not include the specific security requirements or costs as required by OMB budget guidance. They also found

that although security costs were included in their budget submissions, the values were rough estimates with inadequate supporting documentation. OMB is working with all agencies to improve integration and reporting.

10. ***Critical asset prioritization and protection methodologies.***
    The Agency maintains that due to their size (2,800 employees and a $88M FY 2002 IT budget) that "[The Agency] has not required the use of sophisticated methodologies to identify and prioritize our critical assets and infrastructure." They report, and the IG confirms that they have identified two key systems, one of which has a fully tested disaster recovery plan. The recovery plans for the other system are under development. They also have an agency-wide continuity of operations plan, which identifies mission essential functions and documents program priorities. The IG expressed concern that the Agency had not formally implemented Presidential Decision Directive/NSC-63, regarding identification and protection of critical assets. This is a requirement for all Federal agencies, and the IG believes that OPM's overall asset protection would be improved if this step were taken.

11. ***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 reports that the Agency is developing an agency-wide systems development lifecycle methodology. The Agency did not report any examples of measures of performance or actual performance that the Agency could use to ensure the IT security plans are implemented and practiced.

12. ***Integration of IT, critical infrastructure protection, physical, and operational security programs.***
    The Agency has integrated its IT Security with other elements of security through a workgroup lead by the Agency's IT Security Officer, with representation from the program offices responsible for physical and personnel security. The Agency uses this workgroup to coordinate security policy with implementation. The Agency's report claims that these actions will ensure integration of IT security with the protection of critical infrastructure. The IG's findings state that the Agency "has not taken actions necessary to formally implement Presidential Decision Directive-63," which requires Federal agencies to be responsible for protecting their own critical infrastructure. The IG believes that implementing this directive will enhance the Agency's overall IT security.

13. ***Agency methods to ensure contractor services are secure.***
    The Agency indicates that they generally do not rely on contractor provided IT services, but reports that the contractors support data center operations, network management and applications development. Although they do not reference any documented policy or procedures, they give some examples of inspection and monitoring contractor provided services. The IG feels that the Agency, with one exception, has adequate controls for contractor IT services. They believe that supervising contractors in accordance with regulations, providing unique user identification, and requiring access requests and data transmission encryption for

external users, will provide adequate security if controls are implemented to deny former contractors access to systems. Neither the Agency nor the IG discusses the use of other accepted practices such as IT security contract language clauses, personnel background checks, or systematic audits and inspections.

Small Business Administration

1. ***Security funding.***
   The Small Business Administration reports planned FY 2002 funding for IT security and critical infrastructure protection of $2.85M. This funding level comprises 7.3% of their total planned IT portfolio of $39M.

2. ***Number of programs reviewed.***
   SBA reports an inventory of 95 major applications and general support systems, but indicate that only 36% of those systems were evaluated for their annual report. The Security Act and OMB reporting guidance required a review of all programs and systems. The IG evaluation was based on information obtained from audits of 15% of the systems, augmented by further evaluation of the Agency's security program.

3. ***Review and independent evaluation methodology.***
   The Agency used the NIST self-assessment guide as their assessment methodology. The Agency facilitated this process by using information from the current system certifications performed over the past eighteen months as a baseline, and with interviews of individuals knowledgeable about the systems. The IG confirmed the Agency's use of the NIST methodology, and noted that they used general audit methodologies in conjunction with the GAO's Federal Information System Controls Audit Manual.

4. ***Material weaknesses.***
   The IG indicated they had identified deficiencies in IT security, but concurred with the Agency that the financial management and related systems had no material weaknesses that are required to be reported under existing law. The IG cites a number of underlying causes that contribute to deficiencies in IT security, including 39 high to medium risks that have not been satisfactorily addressed, and affect the Agency's ability to protect their information assets.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Agency reports that it has established an agency-wide IT security program, but is still in the process of implementation of the program. The report does not provide measures of performance or examples of actual performances used by the agency to ensure officials are assessing risk, determining appropriate levels of security, maintaining security plans, and testing security controls. It also fails to explain how the agency will motivate program officials to ensure they have effective IT security programs; or how the policies will be enforced. The IG found the Agency had

performed risk assessments on 33 of 95 (35%) of their systems, resulting in the identification of 122 risks, but the Agency had no mechanism to identify which risks had been corrected, mitigated or accepted without correction. Furthermore there is no estimated date for correcting or mitigating the risk. This is of concern because all but one of the systems reviewed for the report were certified and accredited to operate with medium levels of risk exposure. The IG summarized that there are 8 medium/high risks related to monitoring security of systems, 13 for disaster recovery/contingency planning, and 18 for weak assess controls. The IG also noted that a security test and evaluation program needed to be implemented.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Agency's report does not describe the measures of performance used to ensure that the CIO has effectively implemented and maintained security programs and trained employees. The report acknowledges that these are the CIO's responsibility and notes that development and implementation have been delegated to the Agency Computer Security Program Manager. They report that appropriate measures of performance have been established and documented, but the IG disagrees and found that the CIO "should have internal performance measures to manage the program without totally relying upon assessments and audits to provide this service." However, this does not address the issue of measures of performance used by the agency. The IG also challenged the Agency's assertion that training 24% of a group of individuals with significant IT security responsibilities demonstrates adequate training is being affected.

7. ***How the agency ensures employees are sufficiently trained.***
   The Agency reported that it has established annual training programs, but did not provide information on the resources devoted to training making it difficult to assess the adequacy of the Agency's security training. Data was provided for computer security awareness training and the Agency reported that over 90% of their work force was identified as end-users that had received training. They also indicated that 218 individuals with significant security responsibilities received awareness training, but no information was provided on how many Agency employees required or received the advanced training they need to perform their jobs. The IG found that inaccurate records made the training numbers unreliable.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
   The Agency incident response capability is accomplished through a computer emergency response team managed by the Computer Security Program Manager. The report does not discuss the Agency's methods for identifying vulnerabilities, or detecting intrusions, other than to state that the team monitors advisories issued by national computer incident information coordinating centers, and relays that information to affected staff. All employees are assigned responsibility for reporting incidents they encounter. While the Agency may have a functioning incident

response capability, but the only performance information provided was that one incident, an email virus, was reported in the last two years.

9. ***Agency integration of security and capital planning.***
   The Agency reports that their investment management process is used to integrate security into capital planning. The process screens proposals for consistency with the Agency's security plan. They reported that security requirements and costs were reported in capital asset plans included in their FY 2002 budget submission to OMB "where reasonable estimates could be identified." Failure to identify and report security costs for all major and significant IT investments reveals that the Agency has not effectively integrated IT security and capital planning. OMB is working with all agencies to improve this integration.

10. ***Critical asset prioritization and protection methodologies.***
    Although the Agency is not using Project Matrix, its most important elements are contained in the methodology described in their report. Their methodology looks to be a valid approach for the identification and prioritization of critical assets, and uses several sources of information including documentation reviews and interviews with technical staff. The process also uses a software tool that considers a number of factors to establish a risk priority ranking, but did not mention how dependency linkages between assets were determined. The IG expressed concern that a formal review of Agency assets has not been conducted or updated since 1999. Although they found that review to be successful for its time, it did not consider systems that contain sensitive information, are not designated major applications, or fully cover contractor provided services.

11. ***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 report states that the primary measures of performance for the Agency's IT security program are established in a standard operating procedure document. However, no examples of measures of performance are provided as called for in OMB's reporting guidance. The report acknowledges that the Administrator is responsible for establishing management control processes to ensure safeguards, but indicates that this responsibility has been delegated to the CIO. The absence of clearly defined measures of performance in the report raises questions about Agency oversight of IT security. The report states that the Administrator relies on managers, and supervisors, to follow good computer security practices to ensure IT security. While this is a reasonable expectation, it is prudent to use appropriate management tools to verify plans are implemented and practiced. Without verification, the Agency cannot determine if it is complying with the Security Act.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Agency reports, and their IG confirms, that they have a critical infrastructure protection plan. The plan has identified minimum essential critical programs, and identified and conducted vulnerability assessments of cyber-based mission essential

infrastructure. However, the report does not describe how IT security is integrated with physical, operational, personnel, and other types of security.

13. Agency methods to ensure contractor services are secure.

The Agency conducts certification and accreditation reviews of contractor provided IT services to ensure its security. Additional methods used to ensure compliance are service level agreements and audit reviews as needed. The report does not mention the use of other methods such as background investigations, specific IT security contract language, and training. Although these are reasonable practices, the absence of any supporting documentation leaves questions about the comprehensiveness and effectiveness of the certification reviews, assurance that the contractors have reliable backgrounds, and that they are adequately trained.

Social Security Administration

1. Security funding.

The Social Security Administration reports planned FY 2002 funding for IT security and critical infrastructure protection of $38.5M. This funding level comprises 5.2% of their total planned IT portfolio of $742M.

2. Number of programs reviewed.

SSA reports that they reviewed component programs, all four general support systems, and all 12 major applications, but reported on their overall program that covers the entire Agency -- one of the few agencies that defined "program" at such a high level.

3. Review and independent evaluation methodology.

SSA used the NIST self-assessment guide as a framework to evaluate their security program. The majority of responses to the framework questions were based on evaluations of the overall Agency security program with a small subset of the questions answered by “system specific” assessments. The IG found that the assessment efforts were "laudable" in their attempt to baseline security practices, but it did not reach the core issue of security controls effectiveness. The IG concluded that a more constructive review would have included testing to ensure the IT security control environment is operating as intended. The Agency reported that security control testing performed throughout the year formed the basis for its conclusions.

4. Material weaknesses.

The Agency did not report any material IT security weaknesses, based on the Commissioner’s determination that deficiencies were not "significant enough to be reported outside the Agency." The IG reported improvement in the Agency’s information technology security program, but still found numerous weaknesses that had yet to be addressed, many of which have existed for years. The IG "continues to identify weaknesses in the controls for implementing Agency’s IT security program," specifically in training, implementation, and measures of performance to verify the

practice of IT security plans. Both the Agency and the IG note that there is one reportable condition to "strengthen controls to protect its information" under the Chief Financial Officers Act of 1990, Public Law No. 101-576.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans and tested controls.***
   The Agency has recently established measures of performance to ensure they have assessed risks, determined security levels, maintained plans, and tested controls. These measures of performance appear appropriate for the effective management of an IT security program. They include requirements that all sensitive systems are assigned sensitivity levels, are tested annually and prior to going into service, and have plans that are recertified annually. Other goals for the security program are that system downtime for security failures will be less than 2%, all major platforms will be monitored for security, and employee access will be reviewed annually. The report also describes the security practices the Agency intends to follow and use as the basis for their security plans. The Agency did not provide information on the actual performance against these measures.

   The IG found that the Agency "has a fragmented computer security structure that lacks continuity and authority." This deficiency will hamper reporting of Agency performance against metrics and effective oversight of the IT security program. During past audits, the IG has recommended consolidation of security functions. The Agency believes that security ownership throughout the Agency produces a strong program, but is reviewing their structure in response to the IG recommendation. OMB has found that, provided strong central management exists at the Agency level, local ownership, funding, responsibility, and accountability throughout an organization is the most successful approach and is the one envisioned in Clinger-Cohen and the Security Act. Additionally, this approach is a key finding in GAO's 1998 review of information security management in leading organizations. Ultimately, organizational decisions should hinge on whether measurable improvements in program performance will result.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Agency administers its IT security program through a network of security professionals coordinated by the CIO. This group manages security by reviewing systems, making recommendations for improvements, and ensuring they are implemented. The report lists several measures of performance used by the Agency. These include annual awareness training for all employees, a security officer for each organizational component, and systems planning annual reviews. The Agency did not provide data on the actual performance with respect to these measures. To facilitate training the Agency offers 24 specialized security courses for individuals with significant security responsibilities.

The IG characterized the Agency's IT security management framework as "a fragmented organizational structure that lacks continuity," and that the security framework is weakened by several exposures in the information protection control structure. This issue was addressed in item five, above.

7. ***How the Agency ensures employees are sufficiently trained.***
SSA has established annual training programs and is making constructive use of web-based technologies to provide IT security training. The Agency reported that all of their 65,544 employees received some form of training annually, but did not provide any documentation to support this claim. The report does provide a reasonable description of the IT security training offered by the Agency, but does not indicate how many employees should be receiving the various types of training. The Agency did not report IT-security training costs, except to state that $415,000 was spent to train "key security personnel." Without knowing how many people were trained and how many should have been trained, it is difficult for the Agency to assess whether they are devoting adequate resources to training. The IG found that the Agency does not maintain a centralized database to determine who has received training, and it could be several years before they have implemented a training database.

8. ***Agency documented procedures for reporting and sharing vulnerabilities.***
SSA has established an Agency-wide Incident Response Team to deal with attacks and share information with external entities like the GSA's Federal Computer Incident Response Center. The Agency's report provides some examples of documented procedures for how Agency personnel and the Incident Response Team should handle IT security incidents, and does a better job of reporting in this area than many other agencies. The Agency did not report their actual performance in identifying vulnerabilities, dealing with incidents and sharing this information with other organizations. The IG noted that the Agency is reporting on average over 17,000 incidents a year. This is a good indication that the Agency is identifying and sharing information, but does not give a sense of the severity of the incidents or how well they are being handled.

9. ***Agency integration of security and capital planning.***
The Agency reports that IT security is well integrated with the capital planning and investment control process. However, the IG reports that the Agency's capital planning and investment control process did not require: risk assessments for IT projects; integration of tracking; monitoring in-process reviews for performance; capturing different types of IT costs; or establishing post-implementation reviews. The Agency also states that IT security requirements and costs are included in every FY 2002 capital asset plan for significant projects included in their budget submission to OMB. The IG found that the Agency does consider IT security in the budgetary process, but does not track or estimate costs except for projects dedicated to IT security. The IG also pointed out that some reported IT security costs were estimated as a percentage of the project cost, a methodology that requires neither a consideration of IT security requirements nor their integration. OMB is working with all agencies to improve integration and reporting.

10. Critical asset prioritization and protection methodologies.

The Agency was an early adopter of Project Matrix, a methodology they are using to identify, prioritize, and determine the interdependencies of their critical assets. The IG reports that they are in the process of contracting vulnerability analyses, including penetration testing, to complete the first phase of the Matrix review. They are also working to identify public and private sector asset interdependencies. SSA is among the agency leaders in this area.

11. 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 SSA report provides information on the responsibilities of several key IT security managers and professionals, but does not state what measures of performance are used by the Commissioner to ensure the IT security plan is practiced throughout the lifecycle of each system. This is consistent with the IG finding that "No specific measure of performance has been provided by management to determine whether the security plan is practiced," and "Consequently, the Agency cannot demonstrate that it is ensuring the practice of its security plan." The only measures the Agency identified were evaluations and independent reviews, which are necessary, but not sufficient to ensure the practice of the plans and an adequate IT security program.

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

SSA has integrated its IT security program with its critical infrastructure protection program through a system of reviews and evaluations coordinated by a workgroup led by the Deputy Associate Commissioner for Financial Policy and Operations. This workgroup is responsible for the Critical Infrastructure Protection Plan, which addresses IT security, physical security, and continuity of operations. The review process is intended to reveal vulnerabilities and generate recommendations that will have the effect of integrating all aspects of security.

13. Agency methods to ensure contractor services are secure.

The Agency reports that it complies with Security Act and OMB guidance by including standard IT security language templates into contracts that require IT services. While the Agency states that supporting data is available, they did not identify specific measures used to ensure security in this area, e.g., background investigations, training, audits, or other oversight mechanism. The IG found that contract templates did not always contain clauses that would ensure adequate security. Areas that were not covered were specific assignment of security responsibilities and training requirements, incident response handling, and continuity support. The IG also found that post-implementation audits would help ensure adequate security.

Department of State

1. ***Security funding.***
   The Department of State did not answer this question other than to say it would submit funding information to OMB at a later date. Therefore, OMB found it necessary to estimate a total from budget materials regarding individual IT investments provided by the Department. This aggregation may not accurately reflect department-wide funding for IT security. OMB's data shows that the department planned FY 2002 funding for IT security and critical infrastructure protection of $81M. This funding level comprises 9.0% of their total planned FY 2002 IT portfolio of $897M.

2. ***Number of programs reviewed.***
   The Department reported that they reviewed four systems, performed twenty-one computer security evaluations, one independent evaluation. The Security Act and OMB reporting guidance required a review of all programs and systems. The IG conducted forty audits and reported that the Department has 371 systems, 83 of which are characterized as mission critical.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide to review their IT systems. In addition to the NIST guidance, their Diplomatic Security bureau developed a framework based on the Federal Information System Controls Audit Manual to review security aspects of financial systems. The IG used two data collection surveys to perform their review. They also reviewed prior IG and Diplomatic Security bureau reports, and interviewed key officials. They did not conduct any tests of information systems security controls.

4. ***Material weaknesses.***
   Despite a history of weaknesses in their security program and security for individual systems, the Department appears to be in the mode of evolving and developing security plans. While planning is essential, this has been an explicit statutory requirement since the enactment of the Computer Security Act of 1987 and by now, the Department should be executing reliable, established processes including implementing and testing security plans and controls and assessing security performance. The Department has not been effective implementing its IT management controls and has yet to establish a department-wide system that adequately addresses fundamental IT security issues relating to planning, reviews, testing, training, or integration with physical security. Although the IG found that "information security weaknesses continue to threaten Department operations", they did not report any material IT security weaknesses. The IG reported improvement in the Department's IT security program, and that it had recently closed out several material weaknesses that were documented in previous evaluations, but still found numerous weaknesses that had yet to be addressed, many of which have existed for years. The IG audits of the IT security program implementation was mixed,

specifically 26 of 35 posts were adequately training users, but only 10 had adequate procedures in place.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Department did not report the measures of performance used to ensure program officials have fulfilled their responsibilities in this area, but did indicate that their primary vehicle for risk management is certification and accreditation of their IT systems. To determine the appropriate levels of security they rely on System Security Authorization Agreements, and to ensure controls are properly tested they sponsor vulnerability assessments augmented by testing conducted during GAO and IG audits. The IG found that the Department had made significant improvements in the security program by reorganizing in response to IG recommendations, and by the appointment of a CIO and Security Officials for all bureaus and posts. However the measures of performance presented in the IG findings do not support that the Department has been effective in establishing these vehicles. The IG reviewed 16 of the Department's 83 mission-critical systems and found that only 31% had been accredited, 56% had security levels determined, 13% had security plans, 25% had updated/tested contingency plans, and 44% had tested controls. These findings raise concerns over the security of the remaining 67 mission critical systems and the other 288 Department systems. The IG also noted that the Department did not conduct controls testing as part of their work. On a positive note the IG found that 100% of the systems reported having an incident response capability, and 88% reported having the required hardware and software documentation.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The report submitted by the Department does not explain what measures of performance are used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees. The report contains description of plans for what they intend to do and some actions they have taken, rather than descriptions of actual performance against clearly defined measures. The Department reports that they have recently established a System Security Program Plan that contains metrics for assessing performance, but does not provide any examples. The IG added that the Department expects to have metrics defined within two months of their submission of their report. The IG also found that "the Department has not developed information security performance measures to support strategic goals," and go on to state that "without meaningful and measurable performance measures, the Department will be unable to assess the adequacy and effectiveness of information security."

7. ***How the agency ensures employees are sufficiently trained.***
   The Department reports, and the IG concurs, that they have established multiple training computer security initiatives for IT professionals with significant responsibilities. The Department also has policies in place that require appropriate

levels of training for all employees prior to being granted access to computers. They reported FY 2001 spending of $1.1M for security officer training, $656,000 on awareness briefings for all domestic work force employees, and $320,000 for specialized system manager/administrator training for 338 students. Costs ranged from $250 to $2400 per employees in their domestic workforce. However, the need for non-domestic staff training is not provided. The Department reports having trained 13,700 out of 30,000 employees in three years. Annual training and awareness should be the goal. The IG found that the training system does need improving and that "policies and programs concerning information security training awareness were not sufficient to ensure that employees are properly trained to secure the agency's information systems."

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department reported it established formal computer-incident response teams, a network intrusion detection program, and firewalls. They work with both the FBI's National Infrastructure Protection Center and GSA's Federal Computer Incident Response Center to share information on incidents, and are reporting on average 4,500 events a year, of which 600 are referred to law enforcement agencies. This does not include the 400,000 viruses eradicated annually. Threat assessments are conducted by the Department's Cyber Threat Analysis Cell, and are disseminated throughout the organization by weekly reports, advisories, and warnings. Detection, reporting and sharing of vulnerabilities is one of the stronger areas of the Department's IT security program, which appears to be more mature and effective than most other departments and agencies. The IG does not comment specifically on this area other than to note that less than half of the mission critical systems have had security controls tested, and all systems are not scanned for vulnerabilities, leaving open the possibility for undetected intrusions. The IG also found that the Department would benefit from a standardized "Lessons Learned" mechanism to communicate about incidents after they occur. Of special note, the Department has reported that in independent penetration testing, their contractor could not successfully penetrate the Department's networks despite 139 attempts.

9. ***Department integration of security and capital planning.***
Capital planning is integrated with IT security through an IT Planning Board aided by technical/management review advisory groups. This board considers IT security as part of the IT project funding process. The Department reports that they will follow OMB budget guidance for their FY 2003 submission. The Department has not met the requirements of the Security Act or OMB policy.

10. ***Critical asset prioritization and protection methodologies.***
In lieu of a Project Matrix review recommended by OMB, the methodology used by the Department is the Critical Infrastructure Protection Model based on guidance found in Presidential Decision Directive-63, and a categorization process involving three management boards. Details of how the methodology has been implemented are not given in the report and the determination of dependencies between components and links to external systems is not discussed. While the Department's

approach is effective for itself, Project Matrix compiles the data from all agencies to support gap analysis across the government's enterprise. OMB will discuss this with the Department. The IG found that the critical infrastructure protection plan provided a suitable framework for identifying minimum-essential infrastructure. However they also found it is not adequate to address cyber vulnerabilities in its foreign operations or in its interagency connections. The report discusses how the working groups and boards work together to place priority on projects that complement Presidential Decision Directive-63 efforts, but does not describe a systematic methodology that can be used to identify, prioritize and understand the linkages between national and mission-critical assets.

11. ***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 report indicates that responsibility for ensuring that IT security plans are practiced throughout the lifecycle of systems is delegated to the CIO. The report refers to a "number" of high-level measures of performance, but only gives two examples: the material weaknesses reported to Congress via the annual report, and adherence to regulations governing IT security as evidenced in programmatic reviews. The actual performance described for the second measure, adherence to regulations, is not positive. It cites a system's loss of operation for a significant period of time due to failure to implement adequate security safeguards to illustrate the importance of following regulations, but does not indicate how well the Department is performing against this imprecise measure. While additional details are provided in the body of the Department's report, it does fully contradict the IG finding that "the Department has not developed performance measures for its information security program, which are required by both [the] Government Information Security Reform Act and the Government Performance and Results Act."

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department indicates that IT security and critical infrastructure protection are integrated in their Systems Security Program Plan, which has a cross-functional framework that captures all elements of security. Further definition of roles are provided in the Foreign Affairs Manual, and at the implementation level the Regional Security Officers and the Information Systems Security Officers are expected to coordinate their activities. No specific examples of security integration practices are given in the report, and the IG did not comment in this area, so it is difficult to evaluate how effectively different types of security are being integrated within the Department.

13. ***Department methods to ensure contractor services are secure.***
    The Department has taken the approach that since security is the responsibility of all employees regardless of status (civil service, contractor, consultant, etc.) "specific measures for contractor oversight beyond those controls already implemented are deemed unnecessary." This response leaves several questions unanswered. Limitations on government supervision of contractors, and their accountability to

government officials, usually necessitate specific contract language to guarantee compliance with the policies and practices needed to ensure contracted provided services are secure. It is not clear from their report whether or not the Department has the appropriate contract mechanisms, oversight, and audits in place to ensure IT security. Their intention to rely on the same measures of performance that apply to the rest of the work force also raises concerns since those measures have not been well defined.

Department of Transportation

1. ***Security funding.***
   The Department of Transportation reports planned FY 2002 funding for IT security and critical infrastructure protection of $50.9M. This funding level comprises 2.0% of their total planned IT portfolio of $2.51B.

2. ***Number of programs reviewed.***
   The Department reported reviewing 169 application systems, business practices, and security programs distributed throughout the Department's 14 Operating Administrations. These systems include critical safety systems for air traffic management, and search and rescue, and financial systems that process billions of dollars. The Department noted that this is not a complete inventory and the CIO has been assigned the action to provide a consistent comprehensive inventory. The Security Act and OMB reporting guidance required a review of all programs and systems. The IG reported that the Department has over 12,000 computer systems, and more than 150,000 web pages.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide as their assessment methodology. This methodology is derived from the Federal CIO Council's Information Technology Assessment Framework and is recognized throughout the government as an effective analysis tool. However, the IG finds that it is not yet a uniform practice throughout the Department. As mentioned above, four of ten systems evaluated by the IG had not received any reviews in three years, and one bureau was found to have adopted the Department's System Development Life Cycle Management Manual for reviewing its IT initiatives.

4. ***Material weaknesses.***
   The Department reported that they are in substantial compliance with all Federal laws and did not identify any "systemic or structural weaknesses." The Department recognized that material weaknesses had been found by the IG, but indicated that remediation plans will be submitted. The IG found that although the Department has detailed security policies and procedures guidance, they were only partially implemented in the ten major applications evaluated, and not practiced in one of six support systems evaluated. The IG findings discovered weaknesses in virtually every area of IT security including access controls, certification and reporting incidents.

The most serious finding was the IG's ability to penetrate all but one of the general support systems tested. The IG noted that the bureaus acted quickly to correct deficiencies detected by the IG, but progress is slow. As of August 2001 only ten percent of the mission-critical systems have been reviewed for certification. The inability of the Department to detect these problems until an IG investigation, and their persistence over many years raises doubts about the Department's effectiveness in implementing the sound security program guidance they have developed.

5. ***Measures of performance used by the agency to ensure program officials assessed risk, determined security levels, maintained plans, and tested controls.***
   Although the measures of performance used by the agency to ensure program officials are assessing risk, determining security levels, maintaining plans, and testing controls were not specified in the Executive Summary as requested by OMB, some examples are given in the supporting documentation. The metrics used are reasonable for their intended purpose, but only a small percentage listed actual performance. Generally the responses were in the form "assets were identified," rather than a quantifiable measurement like "26 assets identified." The lack of specific data detracts form the creditability of the information. The IG comments that these measures are usually a requirement of IT systems security certification reviews, but less than ten percent of the systems, six percent of the data centers, and 24 percent of the financial systems had been certified as adequately secure. The IG also found that eight of the fourteen bureaus did not conduct security reviews for any systems. These findings and the reported weaknesses in the IT security program indicate that even though measures of performance are in place, the agency does not have adequate information to ensure officials are meeting Security Act requirements.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The report indicates the CIO has requested each bureau to provide measures of performance that will demonstrate the Department's compliance with the Security Act, but they are still in the process of establishing these measures. The report does not provide specific examples of the agency's measures of performance that are used to ensure the implementation and maintenance of the security program, but examples can be found in the supporting documentation. The metrics shown there are appropriate for their intended purpose and a reasonable percentage of the listed actual performance is quantitative. In this instance the Department of Transportation has provided one of the best examples of how measures of performance can help assess a security program's effectiveness. Even though the actual performance in most cases is not satisfactory, having this information is an important step to correcting the situation. Other remaining issues are that the IG found that although the CIO had issued guidance for bureaus to implement security plans, the bureaus' response was incomplete, and the CIO has not performed an assessment of their effectiveness.

7. ***How the agency ensures employees are sufficiently trained.***
The Department has established annual training programs and is making constructive use of web-based technologies and "Security awareness day" events to provide IT security training. The Department reports that close to 99% of their 65,000 employees received general awareness training, however they are not doing as well training employees with significant security responsibilities. Although two bureaus, the Federal Aviation Administration and the Coast Guard, are responsible for 70% of the systems, they have only trained 25% of their Information System Security Officers. The Department is still in the process of identifying all of their system administrators and therefore cannot determine or report how many of their employees require specialized security training. The IG found that of the ones that have been trained, specifics about the training were not available. The Department reported $575,000 in IT security training costs. Cost information was inconsistent across the bureaus making it difficult to assess whether the Department is devoting adequate resources to training or appropriately managing what is provided.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department does not have a fully effective incident response capability. It appears that some progress has been made in this area, but it is limited mostly to internal communications. The IG found that the Department "does not have specific guidelines directing agencies to report security incidents to any central authorities." This finding is supported by the observation that of the 3,500 incidents reported internally, only two were reported to GSA's Federal Computer Incident Response Center. Although the Department has not established consistent documented practices for detection and sharing of incident information, they do have wide spread informal procedures that relies on systems administrators to communicate incidents and distribute information obtained from external sources across bureaus. This process provides some level of protection, but it is compromised by the incomplete training of system administrators, and fails to meet the requirement of the Security Act to communicate vulnerabilities with other departments and agencies.

9. ***Department integration of security and capital planning.***
The Department manages the integration of IT security into their capital planning investment process by delegating the responsibility for the integration to Information System Security Officers within the bureaus, or multiple officials. Each bureau retains the flexibility to define review criteria when approving new initiatives requiring IT security considerations, and many are in the process of developing capital planning review documentation that will emphasize security. However, the response to OMB's question of "Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB?" was that there are inconsistencies between surveys for the Security Act report and the agency's budget submission to OMB. The IG found the inconsistency to be significant. The Department estimated IT security costs to be $44M in the budget submission and $51M in the Security Act report. The IG attributes the difference to inaccurate and unsupported cost estimates. The estimates were generally determined as a percentage of the IT budget, but no details were provided to support the

percentages used, which varied from zero to 25%. The IG noted that the Department "needs to develop better estimation, tracking, and reporting procedures." From the report it appears that the Department has a good understanding of what is required for adequate IT security, but without reasonable and substantiated resource requirements it will not be possible to integrate it with capital planning.

10. Critical asset prioritization and protection methodologies.

The Department reports that they use a variety of methodologies to identify their critical assets. They have used the Presidential Decision Directive-63 as guidance to identify critical infrastructure and officials' individual judgment for mission critical assets. The IG found that the Department did not use any specific methodology such as Project Matrix to identify, prioritize and determine the interdependencies for their critical assets. The IG's independent review disclosed additional critical systems, and concluded that at the present the Department has not fully identified their critical IT assets, and therefore leaves in doubt their ability to protect those assets. Knowing what needs to be protected is one of the first steps in providing protection, and the lack of a methodology that systematically address these issues Department-wide is a serious weakness in the security program. OMB will encourage the Department to use Project Matrix.

11. 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 report does not contain examples of measures of performance used to ensure practice of IT security plans throughout the lifecycle of each system, or actual performance assessed against the measures, as requested by OMB. However, the Department provided supporting documentation with narratives of each bureau's performance against generalized measures of performance for risk analysis, certification activities, rules of behavior, and reviews, but the information is not organized as quantitative measures. The IG believes that periodic system security certification reviews are the key to ensuring the practice of the security plan throughout a system lifecycle, but found that only 10% of the systems had undergone that type of review. The Department plans to certify all systems by 2006, but their incomplete inventory of critical systems prevents them from estimating the resources needed to meet this commitment. Moreover, the proposed timeline to certify the systems (2006) raises a number of concerns and OMB will discuss this with the Department of Transportation.

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

The Department reports that the bureaus are in the process of taking steps to ensure the integration of all aspects of security within their programs and the IG agrees that the Department needs to do a better job of integrating IT and physical security. As an example, the IG cites the Federal Aviation Administration's plans for certifying air traffic control systems do not have adequate provisions for ensuring the physical security of the facilities housing the systems. Vulnerability assessments have been

completed for these facilities, but remediation is not expected until 2006. OMB will discuss this lengthy timeline with the Department.

13. ***Department methods to ensure contractor services are secure.***
The Department relies on various methods including security training, background screening, contract language, and the terms/conditions of the contract to ensure the security of contractor provided services. The IG found that of the Department's 18,000 contractor employees, 85% had received background checks, and the Department was working aggressively to complete the rest. One weakness noted by the IG was that all contracts had not been modified to require background checks. The IG was also concerned that only two of the seven bureaus that allow contractor access to Department systems through direct network connections, were enforcing the policy that requires written assurance from the contractors that their systems complied with Department security requirements.

Department of the Treasury

1. ***Security funding.***
The Department of Treasury reports planned FY 2002 funding IT security and critical infrastructure protection of $174.7M. This expenditure comprises 5.6% of their total planned IT portfolio investment of $3.1B.

2. ***Number of programs reviewed.***
The Department identified 43 major programs, but did not consistently define "program" across their sixteen bureaus. Based on a consistently applied program definition (i.e., a functional area that supports a bureaus mission, with associated IT and budgetary resources) the IG found a total of 39 programs. Of these 34 were reviewed using one or more of the methodologies identified in the next topic.

3. ***Review and independent evaluation methodology.***
The sixteen bureaus of the Department of the Treasury reported using several methodologies to perform their evaluations. They include the Federal Information Technology Security Assessment Framework, the National Security Agency's Information Systems Security Assessment Methodology, the Internal Revenue Service Assessment Framework, and internally developed methodologies based on OMB policy guidance. The IG reported using similar methodologies augmented by reviews of past audits and limited fieldwork to validate information reported by the bureaus.

4. ***Material weaknesses.***
Five of the Department's sixteen bureaus reported weaknesses in the areas of effective oversight, implementation of an entity-wide security program, computer controls, audit monitoring systems, certification of systems, and disaster recover. The IG found that according to their interpretation of the Security Act reporting requirements for material weaknesses, five other bureaus should have reported their

significant deficiencies as material weaknesses. The Security Act specifically limits the definition of "material weakness" to conditions that affect the security of financial systems as covered "under the applicable provisions of law." OMB explained the intent of this provision in its January 2001 Security Act implementing guidance. The Treasury IG and some other agencies and IG's have adopted a broader interpretation that a "material weakness" is any deficiency in policy, procedure or practice that significantly compromises the IT security. The IG justifies the necessity of the broader interpretation as a means to communicate conditions that could adversely affect the Department's ability to meet its objectives and accomplish its mission. Regardless of whether such weaknesses should be reported under other law, they most certainly should be reported or otherwise addressed under the Security Act.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The percentage of systems accredited is the only measure of performance the Department reports using to ensure officials assessed risk, determined security levels, maintained plans, and tested controls. Although this is only one measure, it is more relevant than the information provided by most departments and agencies. However, at the time of their report the IG found that only 18% of the Department's systems had been certified, even less than that Department's modest goal of 20% for FY 2001. The IG points out that this means that 82% of the Department's systems are not accredited, and have been allowed to operate without a reasonable assurance of secure operations or adequate safeguards. This indicates that a majority of the systems fail to meet the requirements of the Department's Security Manual, OMB policy guidance, and the Security Act expectation that departments will ensure the integrity of information systems supporting their operations and assets. With this low percentage of certified systems it is not surprising the IG found half of the bureaus were unable to determine which systems, if any, were fully accredited. Using clearly defined metrics to manage the Department's IT security efforts is a good practice, but the goals should be set to achieve levels adequate to satisfy the intent of the Security Act.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The percentage of systems certified, cited in topic five above, is the only measure of performance used to ensure that the CIO has implemented an effective IT security program. The actual performance against this metric is the same as previously stated, 18% of the Department's systems have been certified. As before this implies that it has not been established whether most systems have in place documented security plans, active testing and self-assessment programs, systematic penetration testing or monitoring and verification of corrective actions. The IG noted an inconsistency in the bureaus acceptance and implementation of the Department's IT security policies and practices, and found that "Treasury bureaus have not effectively implemented performance measures in a department-wide security program." Many bureaus have developed their own measures of performance, but the lack of integration across the

Department compromises their effectiveness. The IG also found that although all bureaus require employees to complete specified training, most bureaus did not address specialized training or adequately track training requirements and attendance.

7. ***How the agency ensures employees are sufficiently trained.***
Fourteen of the Department's sixteen bureaus have reported establishing annual training programs, but the resources devoted to training do not appear to be uniform across all bureaus. Types of training and costs were reported by bureau for fiscal year 2001, but the data was incomplete. The report indicates that $969,000 of the $128M IT security budget was devoted to training activities for a work force of 166,000. No information was provided to identify the relationship between the types of training being given and the requirements for a sufficiently trained staff. The IG observed that although all employees must receive awareness training as a minimum Department-wide requirement, only three bureaus have written policies requiring that employees receive training applicable to their assigned duties. Despite specific training requirements in the Computer Security Act of 1987, six bureaus have not implemented IT security-training policies. The IG also finds that most bureaus have not established measures to track, which employees need or receive, specialized training. As a result of these record-keeping deficiencies, limited evidence is available to show that employees with significant IT security responsibilities are being properly trained to perform their jobs. Many bureaus within the Department appear to be making a substantial effort to train their employees using a variety of methods including classroom and video instruction, distribution of handouts, and online computer training. However, the weaknesses in maintaining training records reported by the IG, and the mixed presentation of the data provided in this report, make it difficult to determine if the work force is being adequately trained to deal with their IT security responsibilities.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
The Department reports a mixed capability for detecting and sharing vulnerabilities across its bureaus. Five bureaus have policies in place for a Computer Security Incident Response Capability, six have procedures for handling incidents, and five have no policy or procedures for handling incidents. The Office of the CIO is acting as the department-wide incident response and information-sharing center. The Department provides GSA's Federal Computer Incident Response Center with a monthly incident report summary based on inputs from each bureau. The data provided by the Department shows a robust incident detection capability with over 25,000 incidents, scan and attempted intrusions detected over a seven-month period, of which fewer than 35 have had serious effect. Most of the bureaus appear to be reporting on a regular basis, with only three of the sixteen, reporting once or less out of seven reporting cycles. The IG noted that the bureaus still do not have consistent incident classifications. Some bureaus decline to report incidents that do not cause serious impact, and thereby fail to share information that can alert other agencies of potential threats. Although the Department lacks a fully operational Department-wide incident response capability, and deficiencies still exist in this area, it has one of the better programs in place among the Federal departments and agencies.

9. ***Department integration of security and capital planning.***
The Department integrates IT security into their capital planning process with an IT Investment Portfolio System that provides a framework for managing IT investments. This policy requires its bureaus to address IT security issues in an investment's selection phase by answering several IT security-related questions for each investment. This is a reasonable and valid approach. The Department implied in their report that security requirements and costs were reported for fifteen of their sixteen bureaus on FY 2002 capital asset plans submitted to OMB, but the IG's analysis indicated that only a few bureaus had reported IT security requirements and costs in their capital asset plans. The IG found that the bureaus were not following Department policy and were not entering data for all projects into the IT Investment Portfolio System. Although the CIO has repeatedly requested the bureaus to comply with Treasury policy over the 21 months prior to the report, the methods used by seven bureaus are inadequate with respect to Treasury guidance. The IG noted that the CIO is taking proactive steps by reminding the bureaus that OMB will not give budget consideration to investments without costs being reflected in their budget submissions.

10. ***Critical asset prioritization and protection methodologies.***
The Department reports that it has elected to use Project Matrix as a methodology for the identification and prioritization of critical assets. The Department reports having completed the first step of Project Matrix, which identified over 1000 information systems, 42 of which were determined to be mission essential infrastructure. The IG found that although the Department had completed the first step, several deficiencies remain to be resolved. These include the need to update the inventory; view the critical infrastructure from a business rather than systems perspective; inadequate training of participants; inconsistent interpretation of critical asset questionnaire; and lack of management support for the effort. The lack of support was reflected in low management priority resulting in insufficient funds and human resources to update and extend the work. The Department reports that additional Project Matrix steps will begin "dependent upon the availability of funding," but did not report whether they had sought such funding in their budget request to OMB.

11. ***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 report does not provide any examples of measures of performance used to ensure practice of IT security plans throughout the lifecycle of each system, or actual performance assessed against the measures, as requested by OMB. The Department reported dissemination of an Information Systems Life Cycle plan (which is not mandatory and has only been adopted by one bureau) and the review of security plans every three years, as the approach used to ensure security plans are practiced. At the bureau level, performance is mixed. The IG noted that although eight bureaus had developed performance measures, the other eight bureaus and the Department had not developed measures to ensure IT security plans are practiced. Furthermore, the IG found that "Specific security plans and structured procedures for systems

development life cycle were largely ignored by the failing bureaus." Even though the IG found many bureaus to be effectively managing this aspect of IT security, the widespread weaknesses in this area indicate insufficient attention is being paid to ensuring IT security plans are being followed throughout the Department.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The Department reports that across all bureaus it has integrated the security disciplines for information technology, physical, personnel, and operational with critical infrastructure protection. The state that they have aligned their security disciplines with the CIO, and plan to do the same within the bureaus. The IG confirmed that a Department-wide security plan has established, but no information was included in the section identified for critical infrastructure protection. The IG also found that guidance to the bureaus on how to develop security policy was out of date and that up-to-date security policies had not been developed for three bureaus.

13. ***Department methods to ensure contractor services are secure.***
    The Department reports that "Designated Security Officials" have been appointed to evaluate and ensure adequate security requirements are imposed on contractors. Their office evaluates contractor provided services for compliance with Federal and Department security requirements. The specific methods reported as being used by the Department to ensure the security of services are periodic audits and requirements for the contractor to support the certification process for systems they designed, provided, operated, or maintain. The report does not refer to any other specific methods, i.e., contract language, contractor employee training, or background investigations, to ensure contractor provided IT services are adequately secure. The IG found that although the Department had established security policies and procedures for its sixteen bureaus and their contractors, only four "have developed security policies that specify the methods to ensure that the services provided by the contractors and other agencies are secure." The IG also found that "although some bureaus conduct vulnerability scans on the networks and perform system penetration tests, comprehensive audit or inspection methods are not employed."

Department of Veterans Affairs

1. ***Security funding.***
   The Department of Veterans Affairs reports planned FY 2002 funding for IT security and critical infrastructure protection of $54.7M. This level of funding comprises 4.6% of their total planned IT portfolio of $1.18B.

2. ***Number of programs reviewed.***
   VA reported reviewing 992 of their major systems. This is among, if not the largest, number of systems reviewed by any agency. These systems support activities distributed throughout five of the Department's six offices and administrations, and

include Veteran's service networks, compensation and benefits delivery, and financial systems, which process billions of dollars.

3. ***Review and independent evaluation methodology.***
   The Department used the NIST self-assessment guide as its assessment methodology. This methodology is derived from the Federal CIO Council's Information Technology Assessment Framework and is recognized throughout the government as an effective analysis tool. Adoption of this guide is the preferred approach for all agencies. The Department automated this process through a web-based survey, which permitted data to be rapidly collected directly from the system owners. The IG used their own methodology that included assessments of security program implementation and Security Act compliance, controls testing, and identifying areas for enhancements. Their evaluations were augmented by scan/probes to detect vulnerabilities and site surveys to investigate electronic and physical security.

4. ***Material weaknesses.***
   VA reported that deficiencies in IT security continue to result in information system security being identified as a material weakness according to the Financial Managers Integrity Act. Audits conducted by the GAO and the Inspector General indicate that deficiencies in security program planning/management, access controls, software change control, service continuity, and segregation of duties are the primary contributors to the material weakness. During the reporting period the Department began using the results of the NIST self-assessment surveys as a tool to effect remediation plans. This is a sound approach.

5. ***Measures of performance used by the agency to ensure officials assessed risk, determined security levels, maintained plans, and tested controls.***
   The Department reported that it has not developed measures of performance to ensure official are assessing risk, determining security levels, maintaining plans, and testing controls. However, this may be an overly self-critical evaluation as VA was one of the few to agencies to provide actual data showing how each component performed with regard to these tasks. The measures of performance provided in the report are based on the NIST self-assessment results. Although performance is not satisfactory, the measures go a long way to assist the Department in evaluating the performance of officials responsible for implementing the Security Act.

6. ***Measures of performance used by the agency to ensure the Chief Information Officer has effectively implemented and maintained security programs, and trained employees.***
   The Department advises that they were unable to provide measures of performance that demonstrate the Department's compliance with the Security Act because their CIO was confirmed just one month prior to submitting their report. They are now in the process of establishing these measures. Although their report does not provide specific examples of performance measures used to ensure adequate security program implementation and maintenance, examples can be found in the supporting documentation. The measures shown are not comprehensive, but are a good start for

their intended purpose. Even though the actual performance in most cases is not satisfactory, compiling this information is important to correcting existing deficiencies. The Department has made more progress than most agencies in this area.

7. ***How the agency ensures employees are sufficiently trained.***
   VA has established annual training programs and is making constructive use of web-based technologies to provide IT security training, however they do not centrally maintain records of who of their 230,000 employees received IT security training. The Department also did not report how many of their employees require specialized security training. They did report that $175,000 was spent on web-based IT security awareness training, less than $1 per employee, and $1.76M on specialized training for employees with significant security responsibilities. However, specifics regarding who has received training and how many employees have been trained were not provided. The lack of specific training information makes it difficult for Department officials to assess whether they are devoting adequate resources to this important area.

8. ***Department documented procedures for reporting and sharing vulnerabilities.***
   VA established a Department-wide Computer Incident Response Center in FY 2000 to deal with attacks and share information with external entities. The Department's Incident Response Center is responsible for notifying organizations within the Department about IT security threats and distributes over 800 security bulletins, alerts, and vendor releases a year. The Computer Incident Response Center is also responsible for reporting incidents externally and reported 442 incidents in the first half of FY 2001, up from 7 in the last quarter of FY 2000. The Department did not report the methods used to detect vulnerabilities, but it is likely that the large increase in reported incidents is due to improved incident detection and communication rather than a breakdown in IT security. The IG found that although most bureaus have incident reporting policies and procedures, some facilities are still not reporting to the incident response center. The Department has made good progress in this area, but the lack of uniform implementation across all bureaus weakens overall effectiveness.

9. ***Department integration of security and capital planning.***
   The Department manages the integration of IT security into their capital planning investment process by requiring that information system security is addressed for all investment projects, or the proposals will not be forwarded for approval. The Department reported that every FY 2002 investment proposal addressed IT security. However, in response to OMB's question in this area, they stated that security costs were not discreetly identified as a separate line item. The Department indicated that they would break this out separately in future budget submissions to OMB. The IG identified 10 new initiatives directed specifically at IT security that will require an expenditure of $114M over the next five years. The Department's report indicates that they have a good understanding of their IT security requirements, but did not provide evidence to demonstrate that IT security was integrated with capital planning. OMB is working with all agencies to improve integration and reporting.

10. ***Critical asset prioritization and protection methodologies.***
    VA established a Critical Infrastructure Working Group comprised of subject-matter experts that rely on their own methodologies to identify the Department's critical assets. Their methodology includes integrating the requirements of existing IT security, contingency, and continuity plans, and Presidential Decision Directive-63 guidance to identify Minimum Essential Infrastructure that support the core mission. The Department chose not to use "Project Matrix" as a methodology and did not explain how they intended to prioritize and determine interdependencies between their critical assets. The result of the Working Group's effort was a Critical Infrastructure Protection Plan that the IG noted was published in 1998. This plan required a comprehensive cyber, physical, and personnel vulnerability assessment that was never completed due to management priorities. The IG also found that the plan had not been updated and "has not been effectively implemented to protect [the Department's] cyber and physical assets."

11. ***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 reports that "Currently, there are no established performance metrics to evaluate the adequacy and effectiveness of incorporating security into the system development lifecycle process" and the IG found that "the Department does not have a System Development Life Cycle for all systems." The Department reports that they are now in the process of working with the Federal CIO Council to develop security metrics.

12. ***Integration of information technology, critical infrastructure protection, physical, and operational security programs.***
    The IG reports that the Department is in the process of developing a plan to ensure the integration of all aspects of security within their programs, but implementation of the integration of IT and physical security with critical infrastructure protection has not occurred. The Department describes how their Office of Computer Security envisions capabilities to enhance IT security, but does not explain how the various aspects of physical and operational security are to be integrated. VA does not provide evidence of having integrated their various security program elements to ensure adequate protection of their mission critical assets.

13. ***Department methods to ensure contractor services are secure.***
    The Department reported that they have policies in place, but other than the requirement for the inclusion of specific contract language in awards, little information is provided on the methods used to ensure the security of contractor provided services. There is no mention of other methods such as security training, background screening, or supplemental independent reviews and audits. Although policies exist, they have not been tested to verify implementation or integrated into the system development lifecycle process.