STATEMENT BY

JOHNNIE E. FRAZIER
INSPECTOR GENERAL
U.S. DEPARTMENT OF COMMERCE

BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 24, 2003

Mr. Chairman and members of the subcommittee, I appreciate the opportunity to appear today to provide the Inspector General's (IG's) perspective on information technology (IT) security in the Department of Commerce.

Commerce's IT systems and the data they process and store are among the most critical assets of virtually all the Department's line offices and operating units. For example, satellite, radar, and other weather forecasting data and systems managed by the National Oceanic and Atmospheric Administration (NOAA) are critical to protecting lives and property; export license data compiled by the Bureau of Industry and Security (BIS) is essential to controlling the export of dual-use commodities to foreign governments and entities; economic indicator data developed by the Economics and Statistics Administration (ESA) has significant policy-making and commercial value and may affect the movement of commodity and financial markets; and data of the U.S. Patent and Trademark Office (USPTO) is essential to administering national and international laws relating to patents and trademarks, promoting industrial and technical progress in the

United States, and strengthening the national economy. Clearly, maintaining the security of Department of Commerce data and systems is of overriding importance to both the agency and the nation. Loss of or serious damage to any one of the Department's critical systems can have far-reaching, long-term, and possibly devastating impacts. Furthermore, without effective IT security, the Department's electronic government initiatives cannot be successful.

State of IT Security at the Department of Commerce

When I first testified on IT security two years ago, I had few favorable observations to share. The Department was striving to improve IT security and make it an integral component of Commerce's business operations. However, our work, augmented at the time by GAO's penetration testing of information systems and networks based in Commerce headquarters, revealed pervasive IT security weaknesses that placed sensitive systems at serious risk. Weaknesses Department-wide prompted us to identify IT security as a top management challenge. Indeed, Commerce exhibited the six common government-wide IT security weaknesses identified by the Office of Management and Budget (OMB) in its FY 2001 report to Congress on government information security reform:

1. Lack of agency senior management attention to IT security.
2. Poor security education and awareness.
3. Failure to fully fund and integrate security into its capital planning and investment control process.
4. Failure to ensure that contractor services are adequately secure.

5. Lack of detecting, reporting, and sharing information on vulnerabilities.
6. Lack of IT security performance measures.

OMB's FY 2002 report to Congress on the state of IT security in the federal government, which was submitted in May, noted that while efforts are still warranted across these six areas, progress is clearly evident, and the federal government is headed in the right direction. I am pleased to report today that Commerce, too, has made progress and is headed in the right direction. But the Department must overcome a history of neglect. In his April testimony before this subcommittee, the Department's CIO, Thomas N. Pyke, aptly stated that Commerce has been "coming from behind" as it strives to implement a comprehensive IT security program. Although significant strides have been made, implementing a comprehensive program to enhance IT security continues to be a top management challenge. As we advised, the Department reported IT security as a material weakness in its *Accountability Report* in both FY 2001 and FY 2002, and we believe it should continue to be reported as such until Commerce systems that are part of the nation's critical infrastructure (national critical systems), as well as those that are mission critical, have been certified and accredited.[1]

USPTO must also address serious IT security issues. As a performance-based organization, USPTO has been submitting its IT security review separate from that of the Department of Commerce. It is also undertaking actions separate from the Department to

[1] Certification denotes that the system's security controls have been tested and found to be adequate; accreditation signifies that the responsible senior manager has formally authorized its operation and accepts any residual risk.

manage IT security, so we reviewed USPTO's IT security program separately in FY 2002. Like the rest of the Department, USPTO is making progress in IT security, but it, too, faces significant challenges. At our urging, USPTO, like the Department, reported IT security as a material weakness in its FY 2002 *Accountability Report*, and we believe it should continue to be reported as such until all USPTO's mission-critical systems are accredited. (We note that USPTO does not have any IT assets identified as part of the nation's critical infrastructure.)

The Six Areas of IT Security Weakness Reported by OMB as They Apply to Commerce

I would like now to address the six areas of weakness reported by OMB as they apply to Commerce, covering their status before GISRA was enacted, the progress that has been made since that time, and the actions Commerce is taking to address its deficiencies. I will then discuss how we perform our evaluations and how our objectivity and independence bring unique insight to this important area.

1. Agency senior management attention to IT security.

Before GISRA was enacted, IT security was not a high priority for senior officials in the Department. This area of responsibility was commonly regarded as belonging solely to the CIOs, who did not treat it as a priority either. And this lack of concern and attention showed. Reflecting a history of neglect, Commerce's IT security program was incomplete, portions that existed were out-of-date, and the program was not enforced. The majority of the Department's IT systems had not been assessed for risk, did not have security plans, and were neither certified nor accredited. This meant that, more often than not, security controls had not been tested, systems were operating without required management authorization, and management officials lacked an understanding of the risks their organizations were incurring by permitting their systems to operate.

Since the enactment of GISRA, the Department's perspective on IT security has changed completely: senior Department management has become intensely aware of and takes very seriously its IT security responsibilities. Under GISRA, IT security became the explicit responsibility of federal agency senior management—the agency head, senior line managers, and the CIO. GISRA charged the Secretary with ensuring the security of information and information systems by promoting security as an integral component of the agency's business operations. Senior Commerce managers were given specific responsibility for protecting the security of operations and assets they control.

As we reported in our FY 2001 independent evaluation, in the summer of 2001 the Department began a concerted effort to improve IT security and make it an integral component of Commerce's business operations. Specifically, the Secretary of Commerce directed secretarial officers and heads of operating units to (1) give IT security high priority, sufficient resources, and their personal attention, and (2) restructure, and thus strengthen, IT management by having a CIO at each unit who reports to the unit head or principal deputy and to the Department CIO, and by increasing the unit CIO's authority over IT resources. We noted that these actions—if accompanied by continued executive-level attention and adequate resources—were important steps in building a more effective IT security program.

Our FY 2002 evaluation confirmed that Department-level executive support for IT security continued. Both the Secretary and Deputy Secretary continued to emphasize to senior Commerce officials the importance of IT security and senior management's responsibility for establishing effective IT security programs in the operating units. They also continued to stress to senior management their leadership role in correcting the problems identified by OIG and GAO evaluations. Our FY 2002 GISRA review found that senior management officials in Commerce's operating units generally were giving IT security their personal attention and were working to ensure that employees understood the responsibilities of their unit's CIO and program officials, as well as their own personal responsibility, for IT security.

However, we still found a need for greater senior management attention in both of the agencies whose IT security programs we reviewed comprehensively in FY 2002—the National Institute of Standards and Technology (NIST) and USPTO. We found that IT security was not receiving adequate senior management attention, and as a result, significant weaknesses existed in planning, budgeting, implementation, review, and oversight. Consequently, we concluded that there had been a lack of follow-through in carrying out such fundamental responsibilities as:

- establishing comprehensive IT security policies and procedures;
- identifying, assessing, and understanding risks to agency IT assets;
- determining IT security needs commensurate with the levels of risk;
- planning, implementing, and testing controls that adequately address risk;
- continually monitoring and evaluating policy and effectiveness of information security practices; and
- developing a capital planning and investment control process and integrating IT security into it.

Since the time of these most recent evaluations, the heads of both of these agencies have stated their commitment to protecting their information assets. In a memorandum to his senior management team, the director of NIST acknowledged his responsibility for the security of NIST's data and IT systems, and directed all members of NIST's upper management to give IT security high priority and to ensure that NIST's policies, procedures, and operational environment are exemplary. NIST has also restructured the CIO's office with the goal of improving its effectiveness.

Regarding USPTO, in response to our evaluation, the Under Secretary of Commerce for Intellectual Property and Director of USPTO began to devote additional attention and resources to this area. In addition to identifying IT security as a material weakness in its FY 2002 *Accountability Report*, USPTO further demonstrated its commitment to improving IT security as part of a new corporate strategy presented in *The 21st Century Strategic Plan*. Referring to the OIG evaluation, the plan states that USPTO is not in compliance with the law and that because IT security has not yet become an integral part of USPTO's business operations, fundamental IT security responsibilities are frequently not carried out. The plan concludes that the implication of not being compliant with GISRA is that neither internal nor external customers can trust USPTO's automated information systems. It further presents tasks, milestones, and a schedule for correcting this problem that are consistent with our recommendations.

2. Security education and awareness.

In our FY 2001 GISRA evaluation, we reported that security training was not conducted on a rigorous or ongoing basis, and none of the operating units was able to give us the information we requested about the number of employees who had received security training or the cost of providing such training. Our FY 2002 evaluation, however, found that significant progress had been made in providing awareness training to IT users. At the direction of the Department's CIO, operating units had provided such training to all employees and contractor personnel either through programs of their own or via web-based training made available by the CIO. The operating units tracked and reported this training to the Commerce CIO and must continue to do so every year.

Operating units are responsible for identifying positions that require specialized IT security training as well as the specific training requirements for those positions. We found that less progress has been made in this area. Training for personnel with significant IT security responsibilities such as system administrators, IT security officers, and contracting officers appeared to be inconsistent and incomplete at the units we reviewed. The Department CIO is addressing this issue by making training more accessible: an enterprise license was acquired for web-based IT security training, which makes both specialized and annual awareness training available throughout the Department. In conducting our ongoing independent evaluation this year, we are finding that some IT security officers still lack a sufficient understanding of their duties and responsibilities, thus highlighting the need for the Department to continue to focus on ensuring that specialized security training is provided to those who need it.

In addition, at the end of FY 2002, the Department CIO sponsored and paid for two important on-site training classes—Principles of Certification and Accreditation, and Roles and Responsibilities of the Designated Approving Authority. These classes covered the methodologies NIST is using to update its federal guideline on certification and accreditation. Although the sessions could not accommodate all personnel who needed them, they were an important step in addressing a critical training area.

3. Funding and integrating security into Commerce's capital planning and investment control process.

By controlling IT spending decisions, the Department and operating unit CIOs can ensure that security is planned at the earliest stages of a system's life cycle. In our FY 2002 independent evaluation, we found that the Department CIO's review and concurrence are required for IT investment decisions affecting all major systems, and—with the exception of NIST—all of the operating units we reviewed (BIS, ITA, NOAA, and NTIA) require unit CIO concurrence for smaller IT investments.

At the Department level, the Commerce Information Technology Review Board (CITRB), chaired by the CIO,[2] was established to support this decision-making function. The Department CIO, with input from the board, provides recommendations to the Deputy Secretary and the Office of Budget on the soundness of the planning for each proposed IT initiative, including the extent to which it addresses Department requirements for IT security and IT architecture. The board seeks to conduct a status review, usually once a year, for approved projects. The CIO, in turn, uses these reviews to recommend whether a project should be continued, modified, or terminated. IT projects costing more than $10 million that require a contract, as well as selected smaller projects, must be reviewed by the board in order for the operating unit acquiring the system to receive a delegation of procurement authority, which is the authority to make contractual commitments. In his FY 2004 and 2005 budget guidance to the operating unit CIOs, the Department CIO emphasized that demonstrating effective IT security is an important factor in the board's review of budget requests.

NIST began to implement an IT capital planning and investment control process in FY 2002; however, our evaluation found that investment decisions could still be made without the review and concurrence of NIST's acting CIO. In responding to our evaluation, NIST noted that its capital investment planning process would be fully implemented in FY 2003, at which time CIO concurrence will be required.

[2] Other members of the board include the Chief Financial Officer and Assistant Secretary for Administration, who serves as co-chair; Deputy CFO; Deputy CIO; the CIOs from NOAA, Census Bureau, NIST, ITA, and, on a rotating term basis not to exceed 2 years, two other operating unit

As part of our FY 2002 independent evaluation, we examined the FY 2003 capital asset plans for 13 major departmental systems—9 of the systems were from NOAA, 2 were from NTIA, 1 was from NIST, and 1 from BIS—to determine whether each capital asset plan (1) specified the system's projected security costs, (2) detailed how funds would be spent, and (3) adequately described the system's security requirements. We found that most plans specified projected security costs, but only a few explained how these funds would be spent. Although most plans described the IT security activities that need to be conducted over the system life cycle, some did not detail specific risks and security controls. We concluded that the operating units need to do a better job of identifying security risks and controls throughout a system's life cycle so that security expenditures can be better developed and justified. The Department CIO is addressing this issue by providing training in the preparation of capital asset plans and specific guidance for completing the security and privacy section. As mentioned earlier, IT security is also given special attention during CITRB reviews.

USPTO carries out its capital asset planning and budgeting process separately from that of the Department. Our FY 2002 evaluation found that USPTO needed to make significant improvements in this area. USPTO had not identified security costs for any individual system in its fiscal year 2002 or 2003 budget submissions. Nor had USPTO conducted an accurate, thorough analysis of existing security needs and the cost of satisfying them in order to develop its budget request. The fiscal year 2002-2007 budget formulation guidance provided by USPTO's Office of the Chief Information Officer did

CIOs; selected operating unit executives as designated by the CIO; Director for Budget; Director for Acquisition Management, and Director for Human Resources Management.

not contain instructions for incorporating security costs into budget requests. In response to this finding, USPTO indicated that the budget system in its CIO office was enhanced to ensure that IT security costs are tracked for each system, and funding for IT security is included in each system's budget plan.

4. Ensuring that contractor services are adequately secure.

This past April, Mark Forman, OMB Administrator for Electronic Government and Information Technology, testified before this subcommittee on the status of the federal government's IT security. While discussing the security of contractor services, he noted that an issue group had been created to review the problem through the Administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board. The issue group recommended use of a government-wide security clause, a recommendation currently under review by the Federal Acquisition Regulatory (FAR) Council.

Of course, the need to safeguard sensitive information and information systems when contracting for services increases as outsourcing increases because the risk of security violations by contractors—whether inadvertent or deliberate—also grows. Thus, I share OMB's concern about ensuring the security of contractor services and believe a FAR clause is needed. I am pleased that my office has been able to help address this issue by having our contracting expert, Karen DePerini, at the invitation of OMB, serve as co-chair of the issue group cited by Mr. Foreman.

Through our FY 2001 independent evaluation, we identified problems with IT security in IT service contracts, resulting, in part, from a lack of sufficient federal and departmental policy and guidance to ensure that contract documents for IT services contain adequate IT security provisions. In FY 2002 we examined this weakness in greater detail: we reviewed 40 of the Department's IT service contracts, including some awarded by USPTO, and found that provisions to safeguard sensitive but unclassified systems and information were either insufficient or nonexistent. Based on the results of this sample, we concluded that the majority of IT service contracts throughout the Department lacked needed IT security provisions. Contracting officers and other acquisition team members need guidance and training, as well as support from technical experts and program officials, to ensure that they prepare and administer IT service contracts in a way that makes clear and enforceable the contractor's responsibility and accountability for safeguarding the government's information assets.

We recommended that the Department of Commerce's Chief Financial Officer and Assistant Secretary for Administration take the necessary actions to ensure that all contracting offices within Commerce include adequate IT security provisions in all IT service contracts to protect the Department's sensitive IT information and assets. Specifically, we urged the Department to establish standard contract provisions for safeguarding the security of unclassified systems and to disseminate clear, detailed policy guidance for acquiring these systems and services.

We further recommended that such a policy require contracting offices—with assistance from the Department's Office of the CIO—to assess the IT security risk associated with the proposed service or system during the acquisition planning phases; identify and include appropriate IT security requirements in specifications and work statements; monitor contractor performance to ensure compliance with IT security requirements; and terminate the contractor's access to systems and networks once the contract is closed out. We also advised the Department to review all current contracts and solicitations for IT services to determine whether IT security provisions should be added to them, even though such revisions might increase contract costs, and to ensure that all procurement personnel have appropriate training in IT security.

The Department is in the process of implementing our recommendations. Contract provisions have been written and are now undergoing departmental review. After the provisions are approved, Commerce plans to provide appropriate training to acquisition staff. The Department's assessment of current contracts found that more than 350 need modification to address the new security provisions. In January, the Department CIO issued a new security program policy, which addresses IT security in contracts and should help ensure that future contracts include appropriate security provisions prior to being awarded.

5. Detecting, reporting, and sharing information on vulnerabilities.

GISRA requires agencies to have documented procedures for detecting, reporting, and responding to IT security incidents. In our FY 2001 independent evaluation, we found that only 4 of 14 operating units—Census, NIST, NOAA, and USPTO—had a formal incident response capability, and that the Department's policy for reporting IT security incidents needed to be revised to specify notification of OIG and to define what constitutes a reportable incident. In FY 2002, the Department established a computer incident response team to support operating units that did not have their own incident response capability, thus ensuring coverage of the entire Department. The team will also be a focal point for obtaining and exchanging best practices and incident response methodologies.

The Department's new security program policy includes improved guidance on incident identification, handling, response, and reporting. It defines the types of incidents that need to be reported and requires each operating unit to submit its response procedures to Commerce's critical infrastructure program manager, located in the Department CIO's office, for review and approval. This requirement will help ensure that all units have documented procedures for reporting security incidents and sharing information about common vulnerabilities. The policy sets minimum requirements for incident response capabilities and prescribes the system-level processes and incident-handling procedures to be performed, including working with OIG investigators and other law enforcement authorities and reporting incidents to the Federal Computer Incident Response Center (FedCIRC). It also establishes requirements for monitoring and detecting incidents, including use of network- and host-based intrusion detection systems, logging tools, firewalls, and other devices, as well as review of audit logs, trouble reports, and information provided by intrusion detection tools.

As Mr. Pyke recently told the subcommittee, Commerce has established a capability to transmit IT security alerts Department-wide at any time and to activate Commerce emergency mobilization plans, as appropriate. To maintain up-to-date corrective patches for known vulnerabilities, the Department established a patch authentication and distribution account under the patch management contract awarded by FedCIRC.

6. IT security performance measures.

Although security plans have been required for federal IT systems since the Computer Security Act of 1987, when I testified two years ago, nearly two-thirds of the Department's systems lacked risk assessments, almost half did not have a security plan, and more than 90 percent were not certified or accredited. These were serious deficiencies that the Department has since been addressing zealously. The table below shows the status of these items, based on Department reporting, between FY 2000 and FY 2003.

Percent of Systems with Risk Assessments, Security Plans, and Certification/Accreditation*

	FY 2000 (percent)	**FY 2001 (percent)**	**FY 2002 (percent)**
Risk Assessments	28	74	94
Security Plans	54	69	96
Systems Certified and Accredited	8	48	77
*Table excludes USPTO's systems.			

Last fiscal year, the Department CIO set September 30, 2002, as the deadline for having approved security plans for all general support systems and major applications. In its fiscal year 2002 GISRA review, the Department reported that of its 609 systems, 94 percent had risk assessments, 96 percent had security plans, and 77 percent were certified and accredited. OMB has established a goal that by the end of 2003, 80 percent of federal IT systems shall be certified and accredited. The Department's goal is to have all national critical, mission critical, and classified systems certified and accredited by the end of this fiscal year.

Performance Measures Do Not Tell the Whole Story; Aggressive Schedules May Actually Weaken the Process

Achieving certification and accreditation for all systems is imperative, and we support the effort to certify and accredit all systems as soon as possible. Our independent evaluations suggest, however, that the Department's aggressive schedule is causing some systems to be certified and accredited in the absence of adequate risk assessments and security plans and without rigorous and effective testing, evaluation, and review processes. While a concerted effort toward certification and accreditation must continue, it is equally critical that the rigor and integrity of certification and accreditation processes be maintained. Otherwise, we may have paper security, but lack true security.

Our concern stems from the fact that our 2002 GISRA review, whose fieldwork we completed in July, found numerous systems operating without required risk assessments, approved security plans, or certification and accreditation. Moreover, some with approved security plans could provide no evidence that a risk analysis—a prerequisite for the security plan—had been conducted. Too many operational systems we reviewed had not been accredited, and many lacked up-to-date security plans and risk assessments. Those that were accredited frequently lacked evidence of the requisite security testing and evaluation, thus diminishing the assurance that accreditation is intended to impart. For example,

- NIST had established an ambitious schedule for accrediting all of its systems by September 1, 2002. As of July, none of NIST's 109 operational systems had a documented risk assessment or an approved security plan, and only two had accreditation. Moreover, the dates by which NIST's offices were to receive a risk assessment methodology had passed, yet the methodology had not been provided. All future dates depended on the risk assessments; thus this delay affected the entire schedule. We were concerned that this aggressive schedule would not permit sufficient analysis, documentation, or review to achieve adequate product content or quality or support meaningful certification and accreditation processes. To address our concern, NIST stated it would have its CIO review all NIST system certifications and accreditations in FY 2003.

- At the time of our evaluation of USPTO, 82 percent of USPTO's 78 operational systems lacked documented risk assessments, and the security plans for 30 percent of those systems were more than 3 years old. None of USPTO's systems had been certified and accredited. In response to our review, USPTO planned to certify and accredit all high-risk systems by the end of FY 2003 and the remaining systems by the end of FY 2004.

- Security plans were provided for all four of BIS systems, which were generally consistent with NIST guidance for content and format, but evidence of a risk assessment was provided for only one system. Although BIS considered the plans approved, it lacked a formal approval process and thus could not validate the approval. None of the systems had undergone security testing and evaluation or been certified or accredited.

- Risk assessments had been performed on the four ITA systems for which we requested documentation. ITA provided two security plans that it considered approved and two draft plans. However, like BIS, ITA lacked a formal approval process. Our review of the two approved plans found them to be generally consistent with NIST guidance for content and format but in need of additional information on rules for using the systems appropriately; they also did not comply with the Department's password policy. Furthermore, none of the systems had undergone security testing and evaluation or been certified or accredited.

- NOAA's Office of Atmospheric Research (OAR) and National Marine Fisheries Service (NMFS) had performed risk assessments on their systems. With one exception, systems belonging to the National Environmental Satellite, Data, and Information Service (NESDIS) and National Ocean Service (NOS) provided hazard information that did not give enough detail to determine needed security controls or conduct certification activities. All the NOAA offices we reviewed had up-to-date security plans whose content and format were generally consistent with NIST guidance and were approved by an IT security officer. However, some of the plans provided by NESDIS, NMFS, and NOS had been updated after the Department issued a revised password policy but did not comply with that policy. Although all NOAA systems we reviewed had current certifications and accreditations, only one had evidence of security testing and evaluation. The seven NESDIS systems we reviewed were accredited after we requested documentation, and the accreditations appear to have been granted in haste. Because we found no concrete evidence to indicate that the appropriate steps had been taken, including security testing and evaluation, the validity of NESDIS' certification and accreditation process is questionable. Since our review, NOAA reported that it has implemented the Department's new password policy and all security plans will be updated to reflect this by September 2003.

- NTIA had conducted risk assessments on the two systems for which we requested documentation and provided security plans for both systems. The content and format of these plans were generally consistent with NIST guidance, but like ITA and BIS, NTIA lacked a formal plan approval process. Neither system had undergone security testing and evaluation or certification and accreditation.

In this year's evaluations, we have found systems whose documented sensitivity levels are understated; their security controls, therefore, are not commensurate with the level of risk. Similar to last year, security plans were developed without current risk assessments, and essential information required for selecting appropriate security controls was missing. Also similar to last year, systems were certified and accredited without testing of security controls.

When implemented properly, the combination of certification and accreditation is a powerful method for helping to ensure that effective management, operational, and technical controls are in place and functioning as intended. Certification actions may be scaled to the level of IT security being evaluated, but they must be sufficient to confirm that the security features of the systems have been implemented as intended and are performing properly, and that the operational sites comply with requirements for physical, procedural, and communications security. This confirmation cannot be achieved without some amount of testing. Unless the certification and accreditation processes are rigorous, the assurances these credentials are intended to impart will be illusory. It is by confirming the substance and quality of such critical processes and controls that IGs can play a uniquely valuable role: performance measures focus the Department on getting the job done; our work helps ensure the job is done right.

The Department recognizes the need for credible IT security processes and products. In FY 2002, to address this need, it began an IT security compliance program, which includes quality reviews of certification and accreditation materials for selected systems.

This year, the Department plans to review these materials for all national critical, mission critical, and classified systems. This review program is a positive step. Nonetheless, our concern remains that aggressive schedules for certification and accreditation may weaken key processes intended to ensure needed IT security.

How We Perform Our Independent Evaluations

GISRA instructed IGs to perform annual independent evaluations of their agency's IT security programs and practices. The evaluation was to include testing the effectiveness of IT security control techniques for an appropriate subset of the agency's information systems. The Federal Information Security Management Act of 2002 (FISMA) similarly requires IGs to perform an independent evaluation, including testing a representative subset of the agency's information systems. OMB Memorandum M-01-08, *Guidance on Implementing the Government Information Security Reform Act,* January 16, 2001, stated that the Act recognizes that not all systems can be reviewed every year and directs IGs to use a sampling of systems to draw conclusions regarding the effectiveness of the agency's overall security program. This guidance also encourages IGs to use reviews performed by other experts in their evaluations.

We have followed this guidance and found it to be both practical and effective. Our independent evaluations consist of a mix of reviews:

- To assess the effectiveness of policy and oversight, we review the IT security program policies of the Department and selected operating units.

- To evaluate operational, technical, and management controls of nonfinancial systems, we review selected IT systems using NIST's *Security Self-Assessment Guide for Information Technology Systems.*

- To evaluate operational, technical, and management controls of financial systems, we use the results of the general control reviews of financial systems conducted by OIG contractors using GAO's *Federal Information System Controls Audit Manual* (FISCAM), which also include limited vulnerability assessments.

- To obtain additional information regarding the responsibilities of the agency head, training of personnel with significant IT security responsibilities, and integration of IT security into the capital planning and investment control process, we interview the CIO and senior IT security officials from the Department and selected operating units, and review pertinent documentation, including selected capital asset plans.

- To obtain coverage of additional operating units and systems, we review the risk assessment, security plan, security testing and evaluation materials (test procedures and results), and certification and accreditation documents for selected systems.

- To extend our coverage further, our evaluation also includes, when available, the results of IT security reviews performed by other parties—typically contractors engaged by the operating units—if we determine, in accordance with OMB guidance, that they are of sufficient quality, applicability, and independence.

Our independent evaluations are conducted by computer scientists and IT security specialists in our Office of Systems Evaluation, several of whom have security certifications and are active on interagency working groups addressing such topics as network security, certification and accreditation, and procurement. But our resources are very limited: we have about four full-time employees performing this work, not including our FISCAM staff and contractor resources. With 14 Commerce agencies and operating units and approximately 600 IT systems, we offer our perspective on the state of IT security in the Department based on our necessarily selective review. Although we do not have sufficient resources or time to validate the specific details of the annual IT security reports submitted by the Department and USPTO, our approach has not only promoted significant improvements in system and program security throughout the Department and USPTO, but has also served as a check and balance on their annual reporting. Our reviews provide objective and independent insight into the state of IT security Department-wide, and virtually every review we have conducted has prompted a major overhaul of policy, oversight, or system security management.

Our budget request for FY 2004 includes those resources we believe are essential for our office to perform further vital oversight tasks. The requested funding level would allow us to perform vulnerability assessments and penetration testing of some nonfinancial systems, a compelling mechanism for demonstrating that vulnerabilities exist and intrusions are possible, and a task that OMB, the General Accounting Office, and we believe should be conducted by IGs. OMB guidance directs agencies to develop plans of action and milestones (POA&Ms) to remediate program- and system-level IT security weaknesses and track each deficiency until it is corrected. According to OMB, an IG-verified, agency-wide POA&M process will be one of three criteria necessary for agencies to improve their IT security status on the Expanding E-Government Scorecard. While we can determine whether the Department's POA&M process is sound, the funding we have requested will allow us to also validate the implementation of a sample of the corrective actions contained in the plans. At present, we are able to track the corrective actions only for deficiencies identified in our financial systems reviews. The increase also will allow us to conduct much-needed additional IT system and operating unit security program reviews.

We believe we have focused and leveraged our efforts effectively. We work closely with the Department CIO to ensure our efforts are complementary and mutually supportive. We also work with operating unit CIOs and, increasingly, with program officials. I believe that GISRA established an effective foundation for improving IT security in the federal government and that FISMA will reinforce this goal. It is a privilege to be able to contribute to improvements in this area, and we hope to do more as time goes on.

This concludes my statement. A list of the reports that are part of our independent GISRA evaluations is included as an attachment. Mr. Chairman, I would be happy to answer any questions you or other members of the subcommittee might have.

ATTACHMENT

U.S. Department of Commerce
Office of Inspector General
Evaluation and Audit Reports
on Information Technology Security

Evaluations	
1	Office of the Secretary, *Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act,* OSE-15260, September 2002.
2	United States Patent and Trademark Office, *Independent Evaluation of USPTO's Information Security Program Under the Government Information Security Reform Act*, OSE-15250, September 2002.
3	National Institute of Standards and Technology, *Additional Improvements Needed To Strengthen NIST's Information Security Program,* OSE-15078, September 2002.
4	United States Patent and Trademark Office, *Stronger Management Controls Needed for the Patent Application Capture and Review Automated Information* System, OSE-14926, August 2002.
5	Office of the Secretary, *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts,* OSE-14788, May 2002.
6	United States Patent and Trademark Office, *Additional Senior Management Attention Needed to Strengthen USPTO's Information Security Program,* OSE 14846, March 2002.
7	Office of the Secretary, *Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act,* OSE-14384, September 2001.
8	Economics and Statistics Administration, *Additional Security Measures Needed for Advance Retail Sales Economic Indicator,* OSE-12754, September 2001.
9	United States Patent and Trademark Office, *Independent Evaluation of USPTO's Information Security Program Under the Government Information Security Reform Act*, OSE-14384, September 2001.
10	Office of the Secretary, *Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened,* OSE-14486, September 2001.
11	Office of the Chief Information Officer: *Use of Internet "Cookies" and "Web Bugs" on Commerce Web Sites Raises Privacy and Security Concerns*, OSE-14257, April 2001.
12	Office of the Chief Information Officer: *Additional Focus Needed on Information Technology Security Policy and Oversight*, OSE-13573, March 2001
13	Office of the Chief Information Officer: *Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed*, OSE-12680, August 2000.

Financial Statements Audits [These audits are performed annually; listed below are only the audits covering FY 2000 and FY 2001.]	
14	U.S. Department of Commerce, *Consolidated Financial Statements, Fiscal Year 2001, Improvements Needed in the General Controls Associated with the Department's Financial Management Systems,* Audit Report No. FSD-14474-2-0001, February 2002.
15	Bureau of the Census, *Improvements Needed in the General Controls Associated with Census' Financial Management Systems,* Audit Report No. FSD-14473-2-0001, February 2002.
16	National Technical Information Service, *Improvements Needed in the General Controls Associated with NTIS's Financial Management Systems*, FSD-14476-2-0001/February 2002.
17	National Oceanic and Atmospheric Administration, Improvements Needed in the General Controls Associated with Financial Management Systems, FSD-14475-2-0001/February 2002.
18	Department of Commerce: *Consolidated Financial Statements, FY 2000*, FSD-12849-1, March 2001.
19	National Institute of Standards and Technology, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12859-1, February 2001.
20	Economic Development Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12851-1, January 2001.
21	Bureau of the Census, *Improvements Needed in the General Controls Associated with Financial Management Systems* and *FY 2000 Penetration Test Results*, FSD-12850-1, January 2001.
22	National Technical Information Service, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12857-1, January 2001.
23	Office of the Secretary, *Follow-up Review of the General Controls Associated with the Office of Computer Services/Financial Accounting and Reporting System*, FSD-12852-1, January 2001.
24	International Trade Administration, *Review of General and Application System Controls Associated with the Fiscal Year 2000 Financial Statements,* FSD-12854-1, January 2001
25	National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12855-1, December 2000.
26	United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12858-1, December 2000.