UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

STATEMENT BY

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

BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

AUGUST 3, 2001

Mr. Chairman and Members of the Committee, I am pleased to appear before you today to discuss the Office of Inspector General's (OIG) work and other activities related to the security and protection of the Department's critical information technology (IT) systems, programs, and activities.

The Department of Commerce has numerous complex computer systems that provide essential services to the public and support critical mission activities, such as the nation's weather services, environmental stewardship, promotion of trade and economic growth, scientific research, and technological development. As the Department's systems have become more interconnected, vulnerabilities have also increased, thus increasing the need to continuously improve IT security measures. Strong IT security measures are vital to (1) protecting the privacy of information, (2) safeguarding the integrity of computer systems and their networks, and

(3) ensuring the availability of services to the American public and other users. I cannot emphasize too much how important these measures are.

Indeed, in our recent *Semiannual Reports to the Congress,* we have identified "Strengthening Department-wide Information Security" as one of the top 10 management challenges facing the Department of Commerce because of that issue's:

1. Importance to the Department's mission and the nation's well-being,
2. Complexity and sizable expenditures, and
3. Need for significant management improvements.

During the past year, we have engaged in a number of audit, inspection, evaluation, and other activities involving Commerce IT security matters—all aimed at strengthening IT security Commerce-wide. We have completed evaluations of the Department's efforts to implement its Critical Infrastructure Protection (CIP) plans. We also have assessed the Office of the Chief Information Officer's (CIO) IT security policy and the effectiveness of its oversight of the Department's IT security program. In addition, we have evaluated the use of persistent Internet "cookies" and "web bugs" on Commerce Internet sites. Furthermore, in support of the OIG's fiscal year 2000 financial statement audits, we have conducted security reviews of the Department's financial management systems and their related networks.

Moreover, assessments of IT security policies and practices are often an integral part of the operational inspections we conduct of Commerce activities, units, and offices domestically and overseas. These inspections are intended to provide operating unit managers with useful, timely information about their operations, including IT security issues. IT security problems have also

been identified through our investigative work. In addition, we have worked closely with many of the Department's key IT managers, top security personnel, and senior program officials in an effort to identify the most critical IT security issues and help craft corrective measures. Let me briefly summarize the results of some of our recent efforts.

Early Progress Made in Critical Infrastructure Protection,
but Planning and Implementation Have Slowed

Last year, we evaluated the Department's CIP plan, identification of minimum essential infrastructure (MEI) assets, and vulnerability assessments of its cyber-based assets. MEI assets are the physical and cyber-based assets essential to the minimum operations of the economy and the government. Our evaluation found that although the Department had made initial progress by developing a Department-wide CIP plan, identifying critical infrastructure assets, and initiating vulnerability assessments, there were several areas that warranted management attention:

- The Department's CIP plan needed to be strengthened because several of its elements were outdated or missing, and important milestones had slipped. The asset inventory, vulnerability assessment framework, and budget estimates included in the plan were not current. The plan also did not include requirements for reviewing new assets to determine whether they should be included as MEI assets, periodically updating vulnerability assessments, or developing a system for responding to infrastructure attacks.

- The MEI asset inventory needed to be reevaluated because of limitations in data gathering. In most cases, asset managers were neither interviewed nor given adequate

guidance before filling out complex questionnaires used to gather asset information, and the officials most knowledgeable about the assets were seldom interviewed because of logistical problems and limited resources. Establishing a reliable MEI inventory is important because it forms the basis for later activities, such as selecting the highest risk assets for vulnerability assessments and taking remedial actions.

- Vulnerability assessments, remediation plans, and budget justifications needed to be completed. Reportedly due to resource constraints, the Department had current vulnerability assessments for less than 10 percent of MEI assets and had not developed any remediation plans.

The CIO's office agreed with our findings and stated that the Department's focus would be on the broad spectrum of IT security, which emphasizes assets critical to the Department's mission and includes most cyber-based MEI assets. Short-term actions were identified to improve guidance to operating unit personnel involved in vulnerability assessments and increase their involvement in the MEI asset inventory, revise the MEI asset list, and evaluate new assets to determine whether they should be included as MEI assets.

Additional Focus Needed on
IT Security Policy and Oversight

The CIO is responsible for developing and implementing a departmental IT security program to ensure the confidentiality, integrity, and availability of information and IT resources. The CIO's responsibilities include developing policies, procedures, and directives for IT security and providing oversight of the IT security programs of the Department's operating units.

We conducted an evaluation to assess the CIO's policies and the effectiveness of his oversight of the Department's IT security program. Our review focused on the CIO's compliance with laws and regulations governing IT security and his actions in recent years to oversee the Department's IT security program.

We found that although in the past IT security did not receive adequate attention, in more recent years, the CIO's office had expanded its focus on and increased the resources devoted to IT security. For example, the office conducted its first Department-wide assessment of IT security planning in 1999 and reviewed operating unit self-assessments in 2000, which resulted in increased compliance with security requirements. Nevertheless, policy and oversight need further improvements. Specifically:

- **IT security policy needs to be revised and expanded**. The Department's IT security policy is out of date because it was developed in 1993 and 1995, prior to a significant revision of OMB Circular A-130, which communicates policy on the security of federal automated information resources. The policy is also missing important components because it has not kept pace with recent trends in technology and related security threats. The Department's policy must be kept current and complete because the operating units use it as the foundation for their general and system-specific policies. We recommended that the CIO's office update and expand its IT security policy as soon as possible.

- **Additional IT security compliance procedures are needed.** Security for many of the Department's systems has not been adequately planned, and security reviews have not been performed. In addition, several operating units do not have adequate awareness and

training programs or adequate capabilities for responding to IT security incidents. The Government Information Security Reform Act (GISRA) requires the CIO's office to conduct annual IT security evaluations in 2001 and 2002 similar to the self-assessments it monitored in 2000. We recommended that the office commit to a program of reviews that extends beyond GISRA's 2-year review requirement. Moreover, the CIO's office should work with the Department's acquisition and budget managers to ensure that IT-related procurement specifications include security requirements, and that funds for meeting these requirements are included in operating unit budgets.

During our evaluation of the Department's IT security policy, we provided the Department with a written analysis that identified weaknesses and deficiencies in the policy, and made recommendations for specific changes to bring the policy into compliance with applicable laws and regulations.

The CIO's office agreed with all of our recommendations and cited a number of corrective actions it planned to take to implement them. Among other things, it agreed to revise, expand, and update the Department's IT security policy; continue its compliance review program beyond the 2-year period required by GISRA; and begin security reviews as soon as possible.

Use of Internet "Cookies" and "Web Bugs"
Raised Privacy and Security Concerns

We evaluated the use of persistent Internet cookies and web bugs by departmental Internet sites, as well as the adequacy of the privacy statements posted on the main web pages of the Department and its operating units. We conducted our evaluation in response to Public Law 106-

554, the Consolidated Appropriations Act of 2001, which required the Inspector General of each agency to submit a report to the Congress disclosing any activity regarding the collection of information relating to any individual's access or viewing habits on the agency's Internet sites.

Persistent Internet cookies are data stored on web users' hard drives that can identify users' computers and track their browsing habits. Web bugs are software code that can monitor who is reading a web page. These technologies are capable of being employed in ways that could violate the privacy of individuals visiting the Department's web sites and can also pose security threats.

Web bugs are considered security threats because they can perform malicious actions, including searching for the existence of specific information, such as financial information, on a user's hard drive, and downloading files from, or uploading files to, a user's computer. A web user would be unaware of the presence of web bugs without using detection software. Even if such software were used, the malicious actions performed by identified web bugs could go undetected.

We found that most of the Department's Internet sites do not use either persistent cookies or web bugs. However, we did find several instances in which persistent cookies were being used without a compelling reason or the approval of the Secretary, as required by Department and OMB policy. We also found a number of web pages using web bugs. At the time we began our evaluation, the Department did not have a policy regulating web bug use, but it promptly developed and issued one when informed of the problem. Finally, we found that many of the operating units' privacy statements did not provide all of the information required by the Department's privacy policy.

We recommended that the Department's CIO direct operating unit CIOs and senior management to implement a strategy to control the use of persistent cookies and web bugs and to certify annually that the operating unit is in compliance with the Department's applicable policies. We also recommended that the CIO direct operating unit CIOs and senior managers to revise their privacy policy statements to make them compliant with the Department's policy. The CIO's office agreed with our findings and worked with us to help ensure that the cookies we had identified were removed. The Secretary of Commerce's new Special Assistant for Privacy is working to remove all web bugs and develop a uniform privacy policy statement.

Systems Security Audits of Departmental
Financial Management Systems Reveal Problems

Our audits of Commerce operating units' financial statements, performed by certified public accounting (CPA) firms under contract with us, include security reviews of the Department's financial management systems and related networks that support the statements. Our CPA contractors use GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide in performing these reviews. FISCAM provides guidance on assessing the reliability of computer-generated data that supports financial statements, including physical security and logical access controls designed to prevent or detect unauthorized access or intrusion into systems and networks.

In 1999 we adopted a systems security review strategy that provides for full coverage of each financial management system and its related networks on a two-year basis. Every two years, a review addresses the six systems security areas identified in FISCAM: (1) *entitywide security program planning and management*, (2) *access controls*, (3) *application software development*

and change control, (4) *systems software*, (5) *segregation of duties*, and (6) *service continuity*. In the alternate years, we routinely conduct penetration testing (in which someone playing the role of a hostile attacker tries to compromise systems security) and application-level testing. Review of the system environment for significant changes and follow-up on open recommendations occurs annually.

The audits of operating units' individual fiscal year 2000 financial statements included reviews of the general system controls over the major financial management systems at the seven data processing locations. In the reports on our audits of the Department's fiscal year 1999 and 2000 consolidated financial statements, we noted that these systems security reviews disclosed weaknesses in controls over major financial management systems at all seven locations that provide data processing support. Specifically, these reviews found that:

1. *Entitywide security program planning and management* needed improvement at all seven locations. This control is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. It is intended to ensure that security controls are adequate, consistently applied, and monitored, and that responsibilities are clear and properly implemented.

2. *Access controls* for both operating systems and the financial management systems needed strengthening at all seven locations, and monitoring of external and internal access to systems needed strengthening at five locations. These controls should limit or monitor access to computer resources to guard against unauthorized modification, loss, and disclosure.

3. *Applications software development and change control* needed improvement at four locations. These controls should help prevent the implementation of unauthorized programs or modifications to existing programs.

4. *Systems software* improvements were needed at four locations. Controls in this area should limit and monitor access to the important software programs that operate computer hardware.

5. *Segregation of duties* improvements were needed at five locations. Appropriate controls in this area include policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets.

6. To ensure *service continuity*, contingency plans needed to be prepared, updated, or improved at all seven locations. Appropriate controls in this area include procedures for continuing critical operations, without interruption and with prompt resumption of those operations, when unexpected events occur.

Of particular note, among the weaknesses identified by the CPA firms in the area of entitywide security program planning and management, was the fact that formal comprehensive security plans either did not exist, were outdated, or were not approved for the major financial management systems and associated general support systems on which the applications were processed. In addition, risk assessments needed to be completed and approved, and security monitoring needed to be performed.

At four locations, penetration testing was also performed on the network that supports the financial management systems to identify weaknesses in access controls. As part of the penetration testing, the CPA firms reviewed the adequacy of access controls, which include logical and physical controls. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access, such as by hackers, to networks, systems, and sensitive files by requiring users to input user ID numbers, passwords, and other identifiers that are linked to predetermined access privileges. Physical controls involve keeping computers in locked rooms to limit physical access. The firms' penetration testing of logical controls found that in some cases:

- Open modems and ports were accessible to potential hackers.
- Sensitive information on websites was readily accessible.
- Sensitive active system services could allow unauthorized access, downloading of files, and gathering of information.
- Firewall configurations could allow a hacker to introduce a destructive virus.

In addition, physical access controls over networks and financial management systems needed strengthening. For example, at one location, automated exterior locking systems had not been installed on doors to restrict access, and the key card lock for the data center's computer room was inappropriately placed on the inside of the door, rather than the outside. In addition, personnel did not consistently lock and secure their work areas. At another location, hardware that processed very sensitive information was located in an area accessible by numerous employees and contractors and was not segregated in an individually secure area.

For fiscal year 2000, the CPA firms concluded that four operating units had system security weaknesses that rose to the level of "reportable conditions." Taken together, these conditions, combined with the Department's lack of an integrated financial management system, constituted a material weakness in the audit of the consolidated financial statements. In our report on the audit of the consolidated statements, we recommended that the CIO's office continue to develop and implement a database for tracking and reporting on corrective actions planned and taken to address the outstanding general controls recommendations. We also recommended that the office review, monitor, and provide guidance to the reporting entities on their corrective actions planned and taken in response to our current and prior years' audit reports on general controls.

We issued audit reports with recommendations to correct the control weaknesses identified at each of the seven data processing locations, and the operating units generally agreed with our recommendations. The Department and its operating units are required to provide us with audit action plans that address each of our recommendations. We have reviewed the plans submitted to date and concur with the actions taken or planned. Moreover, we are in the process of performing our annual follow-up of the adequacy of the corrective actions planned or taken.

IT Security Issues Have Also Been Identified Through OIG Inspections and Investigations

We have also identified IT security issues through our inspections and investigative work. Our inspections unit, for example, conducted a 1999 assessment of the Bureau of Export Administration's (BXA) Export Control Automated Support System as part of a larger review of BXA's administration of the federal export licensing process for dual-use commodities. While we determined that most of the system's general and application controls were adequate, we

found that BXA's IT security controls could be enhanced by improving database access controls, preparing a security plan, performing periodic security reviews, officially assigning the security duties to its security officer, providing all users with current security training, and restricting the number of BXA employees with file manager access. BXA management implemented some corrective actions immediately and agreed to take action on our other recommendations dealing with the IT security of its licensing system.

We are also conducting a series of inspections of the National Weather Service's weather forecast offices (WFOs) that have identified a number of IT security issues that need to be addressed by local managers. Among other problems, we noted that one WFO we visited did not have a designated security officer, and office personnel did not follow the Weather Service's policy on IT security. We found other problems, which I cannot describe in detail in a public hearing, that highlight how vulnerable some systems can be without proper management attention. Fortunately, the Weather Service has greatly improved its IT security both locally and nationally since the start of our review. During the past nine months, we visited two other WFOs. Although we continued to identify some IT security problems, we have found that designated security officers have been named and are receiving necessary training on IT security. More importantly, WFO personnel appear to better understand IT security concepts and requirements.

IT security problems have also been identified through our investigative work. Through our OIG Hotline and other information channels, specific incidents or allegations involving IT security weaknesses, vulnerabilities, or threats have been brought to our attention and examined. For example:

- In one incident, a foreign hacker penetrated a network server and installed software without the knowledge of the system administrator. Had the software been activated, the server would have been prevented from performing its normal network services and would have been one of many computers simultaneously activated to overload a designated Internet site. As a result of the incident, the number of points of access to the network was reduced to a bare minimum, and existing monitoring software was activated.

- In another incident, a hacker caused extensive damage to an operating unit server, and it took more than 5 work days to repair the server and restore operations. Because the software on the server was destroyed, the system administrator was not able to determine how the attack had occurred. Security features were added when the software was restored, to reduce the risk of another shutdown.

- In a third incident, an after-hours contract cleaning employee used a computer that had not been properly secured to gain access to the Internet via a network system and view pornographic materials. Coordination with the contracting officer, property manager, and president of the contract company resulted in the employee's immediate removal from the facility contract and subsequent termination. In addition, the practice of routinely leaving the computer on overnight was discontinued.

Additional OIG Reviews of IT Security Matters
Are Either Underway or Planned

We are currently conducting IT security evaluations related to (1) the Economics and Statistics Administration's and the Census Bureau's preparation and release of the Advance Retail Sales

Principal Economic Indicator, (2) the Department's classified information systems, and (3) the Department's IT security program and practices, as required by the Government Information Security Reform Act.

The objective of our security evaluation of the Advance Retail Sales indicator is to determine whether adequate internal controls and system safeguards are in place to prevent the unauthorized disclosure or use of the economic indicator data before its release to the public. We have found that employees dealing with the indicator do not always have appropriate background investigations and that their positions are not always assigned the appropriate level of risk as required by Title 5, Part 731, of the Code of Federal Regulations and OMB Circular A-130. In some instances, the Department's records did not identify the type of investigation done, if any, for personnel working on Principal Economic Indicators. We also noted a lack of guidance from the Office of Human Resources Management, as well as from the Office of Security, suggesting that the problems associated with assigning appropriate risk levels to positions and ensuring that background investigations are performed may exist throughout Commerce. We are conducting additional work to examine this issue.

Our review of the Department's classified information systems will assess the adequacy of its policies for protecting classified information and the effectiveness of its oversight of these systems.

The GISRA-mandated review is the annual evaluation of the Department's IT security program and practices. This evaluation will incorporate information from our security reviews, as well as results of related evaluations performed by operating units, GAO, and contractors. We are also continuing our security reviews of Commerce's financial management systems and related

networks as part of our fiscal year 2001 financial statements audits. These reviews will be in line with our IT security review strategy and will include penetration testing of the U.S. Patent and Trademark Office and FISCAM reviews for the other operating units.

The need for the OIG to provide oversight and evaluation of IT security will be increasingly critical in the coming years. Our independent evaluation of the Department's IT security program being performed under GISRA and our security reviews of the Department's financial management systems show that although the Department is giving greater attention to IT security, serious issues remain to be resolved. These issues appear to be the result of an earlier lack of attention to IT security, limited resources, and an environment in which the risks, threats, and vulnerabilities have continued to escalate in number and complexity. The weaknesses identified by GAO's recent network vulnerability analysis of the Department underscore our concerns.

In our independent GISRA evaluation for the next fiscal year, we plan to evaluate the effectiveness of operating unit IT security programs and to conduct security evaluations of specific general support systems and major applications. We will use the findings of our current GISRA evaluation and of GAO's security audit to assist us in identifying specific operating units, general support systems, and major applications to evaluate in the future.

Cooperative Efforts Needed to Address
IT Security Weaknesses

I am pleased to note that, just last month, my office entered into a memorandum of agreement with the Department's Office of the CIO and Office of Security to define our respective roles and

responsibilities relating to the development, implementation, and management of the Commerce IT security program. This agreement is intended to promote a partnership among the three offices that both ensures complete coverage of IT security matters and prevents wasteful duplication of effort.

Under the agreement, the CIO's office has the basic responsibility for developing and implementing the Commerce-wide IT security program, which includes developing IT security policies and procedures, promoting IT security awareness and training, serving as the Department's critical infrastructure assurance officer, and convening a meeting of the incident response group when incidents or intrusions occur. Commerce's Office of Security has the primary responsibility for security for the Department's classified systems and, in conjunction with the Department of State, for IT security at Commerce overseas posts. My office is responsible for conducting investigations of IT incidents and intrusions, and for conducting reviews of the Department's IT security program and individual systems, including the annual independent evaluations of the program required by GISRA.

In closing, it is clear that cooperative, continuous, and concerted efforts are needed by each of us—and I mean each of us—if we are to address IT security weaknesses. These efforts are needed if we are to have any chance of staying at least one step ahead of the hackers and others that see IT security as some sort of cat-and-mouse game.

I am confident that the senior management of the Department and its operating units increasingly recognize the need to take a proactive approach to do this. For example, the Secretary's recent directive increasing the authority of operating unit CIOs and making them a more integral part of the management team is an important initiative. Likewise, the recent appointment of a Senior

Advisor to the Secretary for Privacy should be instrumental in addressing such issues as cookies, web bugs, and other security/privacy matters. And program officials are also being strongly reminded that they too have key IT security responsibilities and need to work closely with operating unit CIOs and security officials to ensure an effective security program.

We intend to continue our partnership with all of these managers by identifying weaknesses and potential vulnerabilities in IT security and by searching for ways to improve it. Through this relationship, I believe we can help strengthen IT security within the Department.

~ ~ ~ ~ ~

This concludes my statement. A list highlighting some of the reports we have issued that address IT security issues is included as an attachment. Mr. Chairman, I would be happy to answer any questions you or other members of the Committee might have.

ATTACHMENT

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

Evaluations	
1	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
2	Office of the Chief Information Officer: *Additional Focus Needed on Information Technology Security Policy and Oversight*, OSE-13573, March 2001
3	Office of the Chief Information Officer: *Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed*, OSE-12680, August 2000
4	Bureau of the Census: *Computer Security for Transmission of Sensitive Data Should Be Strengthened*, OSE-10773, September 1998
Financial Statements Audits [Note: These audits are performed annually; listed below are only the reports covering FY 2000. In addition, the reports on security reviews are not publicly available documents.]	
5	Department of Commerce: *Consolidated Financial Statements, FY 2000*, FSD-12849-1, March 2001
6	National Institute of Standards and Technology, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12859-1, February 2001
7	Economic Development Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12851-1, January 2001
8	Bureau of the Census, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12850-1, January 2001
9	National Technical Information Service, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12857-1, January 2001
10	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
11	International Trade Administration, *Review of General and Application System Controls Associated with the Fiscal Year 2000 Financial Statements*, FSD-12854-1, January 2001

12	National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12855-1, December 2000
13	United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with Financial Management Systems*, FSD-12858-1, December 2000
Inspections	
14	National Oceanic and Atmospheric Administration: *San Angelo Weather Forecast Office Performs Its Core Responsibilities Well, but Office Management and Regional Oversight Need Improvement*, IPE-13531, June 2001
15	National Oceanic and Atmospheric Administration: *Raleigh Weather Forecast Office Provides Valuable Services, but Needs Improved Management and Internal Controls*, IPE-12661, September 2000
16	Bureau of Export Administration: *Improvements Are Needed to Meet the Export Licensing Requirements of the 21st Century*, IPE-11488, June 1999
17	Office of Security: *Vulnerabilities in the Department's Classified Tracking System Need to Be Corrected*, IPE-11630, March 1999