U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Office of the Secretary

FY 2004 Independent Evaluation Of the Department of Commerce's Information Security Program Under the Federal Information Security Management Act for FY 2004

Final Report No. OSE-16954/October 2004

Office of Systems Evaluation

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

OCT 6 2004

MEMORANDUM FOR: Theodore W. Kassinger
Deputy Secretary

FROM: Johnnie E. Frazier

SUBJECT: *FY 2004 Independent Evaluation of the Department of Commerce's Information Security Program Under the Federal Information Security Management Act for FY 2004*
Final Inspection Report No. OSE-16954

This memorandum transmits our independent evaluation of the Department of Commerce's information security program, as required by the Federal Information Security Management Act (FISMA). FISMA mandates two annual reviews of an agency's information security program: one conducted by the agency itself and a second, independent evaluation performed by the agency's Office of Inspector General (OIG). We prepared our evaluation report in accordance with the Office of Management and Budget's (OMB's) FY 2004 instructions and prescribed reporting template.

The objective of the FISMA evaluation was to determine whether the Department's information security program and practices comply with the act's requirements, and thereby protect the information and information systems on which the federal government depends.

As our report shows, the Department has continued to make progress on improving information security during this past fiscal year. We were pleased to note, for example, that consistent with FISMA goals, (1) no operating unit can make a major IT investment without the Department CIO's review and concurrence, (2) the inventory of major IT systems continues to be updated, (3) a process is in place for documenting known IT security weaknesses and managing remediation efforts, and (4) IT security awareness training is provided to virtually all employees.

However, we found persisting areas of weakness, most notably in critical system certifications and accreditations (C&As). Certification is the detailed testing and evaluation of information systems to ensure that appropriate security controls are implemented and working as intended; accreditation is the formal authorization by management for system operation, including an explicit acceptance of risk. Through accreditation, senior agency officials formally become accountable for the security of

systems for which they have budget and operational authority. Unfortunately, our recent review of a random sample of 24 certification and accreditation packages throughout Commerce for systems deemed national-critical (part of the critical infrastructure) and mission-critical identified serious deficiencies in risk assessments, security plans, and testing and evaluation of security controls. Testing and evaluation is a particular concern because unless security controls are thoroughly tested and deficiencies documented and appropriately addressed, there is little, if any, assurance that the Department's IT assets are protected by effective information security safeguards as envisioned by FISMA. But our recent review of C&A packages revealed that too many IT systems—including those for systems that are part of the critical infrastructure—have not undergone adequate testing.

The Department reported information security as a Federal Management Financial Integrity Act (FMFIA) material weakness in its *Performance & Accountability Report* for the past 3 fiscal years. In FY 2002, we advised the Department and USPTO—and they agreed—that the material weakness should remain until all national-critical and mission-critical systems have certifications and accreditations of sufficient content and quality to provide reasonable assurance that these systems have appropriate and well-functioning security controls and that accrediting officials authorize operations only after residual risks have been explicitly identified.

We reported serious shortcomings in the Department's C&A materials in FY 2003, but noted that USPTO was using a disciplined C&A process that includes rigorous testing of security controls. (We address USPTO's C&A process separately because, as a performance-based organization, it submits its *Performance and Accountability Report* separate from that of the Department.) However, USPTO's material weakness remained in FY 2003 because it was not able to certify and accredit all of its mission-critical systems. (USPTO has no national-critical systems.) Based on our recent work at USPTO, we are pleased to note that its information security program has continued to progress. In particular, USPTO completed certification and accreditation of all of its systems this fiscal year using the same disciplined process as last year. As a result, you can have increased confidence in the security of USPTO's IT systems. Therefore, we consider its material weakness resolved.

The good news is that USPTO is not alone. Specifically, we found that the Bureau of Economic Analysis and the Office of the Secretary do not have a material weakness either. Improvements in other operating units' C&A packages are also apparent. Unfortunately, our review found serious deficiencies for eight other operating units, including Census, NIST, and NOAA. These deficiencies include such things as (1) risk assessments that do not provide a sufficient identification of threats, vulnerabilities, and risks; (2) security plans that do not adequately describe the system environment, interconnections, and/or sensitivity of the data that is processed; (3) certification testing and evaluation that does not ensure that security controls are implemented correctly and operating as intended; (4) contingency plans that are incomplete and fail to provide adequate recovery procedures; and (5) weaknesses in system security controls that, through the C&A process, should have been identified, analyzed, documented, and

corrected. Therefore, in our judgment, the Department has not yet made sufficient progress to resolve the material weakness. Given that more than half of the Department's nearly 500 systems are national or mission critical, and many of these are large and complex, sufficient certification and accreditation requires meticulous effort and is a challenge too often underestimated.

As part of the FISMA process, we continue to work closely with the Department's CIO and his staff to promote information security improvements. As such, we are aware that he has placed considerable management attention and resources on improving system certification and accreditation in FY 2004. Moreover, in our numerous discussions with the CIO and his staff, we have been advised of his plans to maintain this focus in FY 2005, as evidenced by efforts already under way to address the deficiencies we identified in this year's independent assessment. The CIO has also initiated action to improve the handling of computer security incidents throughout Commerce in response to our concerns and recent report on this topic. Finally, the Secretary has underscored the Department's commitment to information security and again issued a memorandum this year (dated June 29, 2004) directing secretarial officers and heads of operating units to continue to give this area high priority. We are confident that sustained senior management focus on IT security will result in continuing improvement in the Department's IT security program and more secure IT systems in the coming year.

OMB's reporting instructions call for agency heads to transmit their OIG's report as a component of their agency's FISMA report. Accordingly, we have included a copy of the OIG portion for inclusion in Commerce's report.

Please do not hesitate to contact me on (202) 482-4661 if you would like to discuss our FISMA reports or any other aspect of Department's information security status, or have your staff call Judith Gordon, Assistant Inspector General for Systems Evaluation, on (202) 482-5643.

Attachment

cc: Thomas N. Pyke, Jr., Chief Information Officer, U.S. Department of Commerce

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		**A.1.b. FY04 Systems**		**A.1.c. FY04 Contractor Operations or Facilities**		**A.2.a. Number of systems certified and accredited**		**A.2.b. Number of systems with security control costs integrated into the life cycle of the system**		**A.2.c. Number of systems for which security controls have been tested and evaluated in the last year**		**A.2.d. Number of systems with a contingency plan**		**A.2.e. Number of systems for which contingency plans have been tested**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
BEA			2				2	100.0%	2	100.0%	2	100.0%	2	100.0%	2	100.0%
BIS			1				0	0.0%	1	100.0%	1	100.0%	0	0.0%	0	0.0%
Census		1	2				0	0.0%	2	100.0%	2	100.0%	1	50.0%	0	0.0%
EDA			1				0	0.0%	1	100.0%	1	100.0%	1	100.0%	0	0.0%
ESA			1				0	0.0%	1	100.0%	1	100.0%	1	100.0%	0	0.0%
ITA																
MBDA																
NIST		1	3				0	0.0%	3	100.0%	3	100.0%	3	100.0%	1	33.3%
NOAA		1	8				0	0.0%	8	100.0%	8	100.0%	6	75.0%	0	0.0%
NTIA			1				0		1	100.0%	1	100.0%	0	0.0%	0	0.0%
NTIS			1				0	0.0%	1	100.0%	1	100.0%	1	100.0%	0	0.0%
OS		1	1				1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
TA																
USPTO		1	3				3	100.0%	3	100.0%	3	100.0%	2	66.7%	1	33.3%
Agency Total		**5**	**24**				**6**	**25.0%**	**24**	**100.0%**	**24**	**100.0%**	**18**	**75.0%**	**5**	**20.8%**

Comments: **(A.1.a.)** Program reviews: 1. Census IT security program; 2. OS (Office of the Secretary)--Department-wide computer incident response capability; and 3. NIST, NOAA, and USPTO--selected aspects of IT security program through discussion with agency CIO and senior IT security officials and limited documentation review.

(A.2.a.), and (A.2.d.-A.2.e.) All 24 systems we reviewed have been certified and accredited and were identified by the bureaus as having contingency plans; 19 contingency plans were identified as tested. We did not count these items in the above performance measures, however, when our review found deficiencies in their quality or completeness such that they do not meet the minimum standards contained in Departmental IT security policy o NIST SP 800-26. Our assessment of the number of systems certified and accredited and of contingency plans is based on our review of system C&A documentation and any other documentation provided by the bureaus, as well as, in some cases, follow-up discussions with certifying officials and IT security officers. While Commerce has placed considerable emphasis on improving these areas in the past year and has made significant progress, additional improvements are needed.

A.3	
A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.	
Statement	**Evaluation**
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Mostly, or 81-95% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Almost Always, or 96-100% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Mostly, or 81-95% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Mostly, or 81-95% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Frequently, or 71-80% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments: (A.3.a.) OIG evaluated this statement for Census, NIST, NOAA, and USPTO. For contractors and other government agencies identified by Census and USPTO as providing services requiring review, reports on the results of the reviews were provided. NIST and NOAA indicated that they receive no services requiring review. We did not validate whether all contractor- and other government agency-provided services needing review were identified.

(A.3.d.) Although an inventory of major IT systems is maintained and updated semiannually, our review of security plans found that identification of interfaces between other systems and networks is incomplete.

(A.3.e.) The CIO's office seeks our input in developing and updating policy and guidance for inventory management, provides a copy of the most current inventory, and keeps us apprised of its efforts to validate the inventory. However, OIG has not independently validated the inventory.

(A.3.f.) The numbers appear generally to be accurate. We have concerns, however, about whether all contractor operations or facilities have been identified.

(A.3.i.) The senior IT security officer has direct access to the CIO. For supervisory purposes, she reports through the Director, Office of IT Security, Infrastructure, and Technology to the CIO.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

16954
, 2004

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

Bureau Name	FY04 Significant Deficiencies			
	Total Number	Total Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
BIS	*			
Census	*			
EDA	*			
ESA	*			
NIST	*			
NOAA	*			
NTIA	*			
NTIS	*			
Agency Total	1	1	Deficiencies in system certification and accreditation.	Yes

Comments: * We reviewed a random sample of Commerce's certification and accreditation (C&A) packages for 24 certified and accredited national-critical and mission-critical systems. C&A packages were selected from all bureaus that have national-critical and/or mission-critical systems: BEA, BIS, Census, EDA, ESA, NIST, NOAA, NTIA, NTIS, OS, and USPTO. Our sample included 50% of the Department's 16 unclassified national-critical systems and 7% of its 231 unclassified mission-critical systems (based on Commerce's July 2004 system inventory). With the exception of BEA and OS's C&A packages, our review continued to identify significant deficiencies. Serious weaknesses were identified in all national-critical systems, with the exception of BEA's. (Census, NIST, and NOAA also have national-critical systems.) Our response to Question C.2 provides specific information about the deficiencies. POA&MS are developed for the deficiencies OIG identifies and about which we make formal recommendations in evaluation reports. However, while POA&MS address some deficiencies identified by the bureaus in conducting C&A, the bureaus have generally not identified the weaknesses we found and thus many are not yet documented in POA&Ms.
Although Commerce continued to have significant C&A deficiencies in FY 2004, as noted previously, progress has been made, and the Department's CIO and Commerce bureaus are continuing to invest a substantial effort and resources in improving this critical area.

As a performance-based organization, USPTO submits its *Performance and Accountability Report* separate from that of the Department. Therefore, we address USPTO's C&A process separately. In last year's FISMA evaluation, we noted that USPTO was employing a disciplined certification and accreditation process that included rigorous testing of security controls. But because of the security weaknesses being identified by the certification process and the lack of final accreditations for all but one of its mission-critical systems, we advised USPTO to report information security as a material weakness for FY 2003, and USPTO did so. USPTO completed certification and accreditation of all of its mission-critical systems this fiscal year, maintaining its disciplined C&A process for the systems we reviewed. In our judgment, USPTO has resolved the material weakness.

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Sometimes, or 51-70% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Rarely, or 0-50% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always, or 96-100% of the time

Comments: (C.1.a.) All weaknesses known to the Department are reported on POA&Ms. However, for the systems we reviewed, we found that IT security weaknesses identified in C&A materials were frequently not included in system or bureau POA&Ms or documented as residual risks accepted by the accrediting official. Weaknesses identified in self assessments usually are documented on POA&Ms, but bureau self assessments generally do not adequately identify weaknesses.

(C.1.b. and C.1.d.) Program officials and CIOs develop, implement, and manage POA&Ms when IT security weaknesses have been identified and brought to their attention. As noted in our comment on C.1.a., weaknesses identified in C&A materials were not always included in POA&Ms or documented as residual risks accepted by the accrediting official for the systems we reviewed.

(C.1.f.) The POA&M is authoritative for the Department. However, because we have found the C&A process and bureau self assessments generally do not adequately identify weaknesses and weaknesses identified in C&A documentation are not always recorded in POA&Ms, OIG places greater reliance on our own independent reviews for identifying weaknesses.

C.2 OIG Assessment of the Certification and Accreditation Process
Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Comments: The Department's policy and guidance generally serve as a sufficient basis for an effective C&A process, although requirements for testing must be clarified. However, our in-depth review of a random sample of C&A packages for 21 national- and mission-critical systems throughout the Department found significant weaknesses. Of the 21 packages we reviewed, (1) 10 had risk assessments that did not provide a sufficient identification of threats, vulnerabilities, and risks; (2) 8 had security plans that did not adequately describe the system environment, interconnections, and/or sensitivity; (3) 18 did not provide evidence that certification assessment and testing were adequate to ensure that security controls were implemented correctly and operating as intended; (4) 5 did not have contingency plans that were complete and provided adequate recovery procedures; (5) 12 did not have evidence of contingency testing; and (6) 15 did not document all weaknesses identified through C&A in POA&Ms.	Poor
Comments: Our review of 3 USPTO C&A packages found that USPTO's C&A process generally provides adequate assurance that security controls are appropriate, implemented correctly, and performing as intended. A particularly effective aspect of USPTO's process is the use of certification testing and risk assessment to identify and correct IT security weaknesses. USPTO still needs to ensure that all system components are identified and tested and that all systems have contingency plans and these plans are tested.	Good

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	No	
a. Windows XP Professional		
b. Windows NT		
c. Windows 2000 Professional		
d. Windows 2000		
e. Windows 2000 Server		
f. Windows 2003 Server		
g. Solaris		
h. HP-UX		
i. Linux		
j. Cisco Router IOS		
k. Oracle		
l. Other. Specify:		
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?		

N/A

Comments: The Department's information security policy requires configuration management (CM) of all general support systems and major applications, including a description in system security plans of how CM is to be implemented on each system. Also, the policy recommends that employees consult various sources for information on secure operating system configurations such as the Department of Defense's Security Technical Implementation Guides. In July 2004, the Department subscribed to the Defense Information System Agency's Gold Disk configuration and patch management service, which provides products that automate the remediation of configuration vulnerabilities and aid in establishing and maintaining configurations. Bureaus may use these products at their discretion. However, the CIO has not yet implemented agencywide policies that require detailed, specific security configurations.

Our review of Census, NIST, NOAA, and USPTO found that NIST, NOAA, and USPTO have configuration requirements, which address patching of security vulnerabilities. However, we have not evaluated whether these units have developed configuration requirements for all operating systems and applications that need them, nor have we assessed the extent to which the configurations have been implemented.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Rarely, or 0-50% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Rarely, or 0-50% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Rarely, or 0-50% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	19	83%

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

IT security policies, user authentication, awareness and specialized training, limited use of insecure protocols and implementing SSH, SSL, role-based access, applying ACLs to routers and file systems, firewalls, host- and network-based IDS sensors, encrypted network communication links and sessions, anti-virus protection, VPNs, and PKI.

Comments: (E.1.a. & c.) Our evaluation of the Department's computer incident response capability found that bureau incident response reporting was incomplete and inconsistent, with detected incidents frequently not reported. In responding to our evaluation, the Department CIO stated that policies and procedures will be revised to provide for prompt reporting, and bureau compliance will be reviewed. We note that the Department also identified the need to improve incident response policies and procedures and documented this weakness in its POA&M in FY2004.

(E.1.b.) Few compromises were reported to OIG's Office of Investigations, and the Department's FISMA reporting shows that few were reported to law enforcement.

(E.2.a.) Response based on 23 systems; one of the 24 systems was a major application running on a different general support system that was not included in our sample.

(E.2.b.) Response based on our review of 24 systems.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			**F.2. Number of systems affected, by category, on:**		
	F.1.a Reported internally	**F.1.b. Reported to US-CERT**	**F.1.c. Reported to law enforcement**	**F.2.a. Systems with complete and up-to-date C&A**	**F.2.b. Systems without complete and up-to-date C&A**	**F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?**
	Number of Incidents	**Number of Incidents**	**Number of Incidents**	**Number of Systems Affected**	**Number of Systems Affected**	**Number of Systems Affected**
I. Root Compromise						
II. User Compromise						
III. Denial of Service Attack						
IV. Website Defacement						
V. Detection of Malicious Logic						
VI. Successful Virus/worm Introduction						
VII. Other						
Totals:	*	*	*	*	*	*

Comments: * At the time of our evaluation, incidents were not categorized in this way. However, our review of the Department's computer incident response capability found that most bureaus identify few incidents, and noted this was a consequence, in part, of poor incident detection techniques. We found that system administrators and IT security officers need to improve their intrusion detection approaches and obtain additional specialized tools and training. In responding to our evaluation, the Department CIO identified actions that will be taken to address these issues including (1) improving the IT security policy and procedures for reviewing network log device information, (2) obtaining automated tools, and (3) providing training to IT security personnel.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
9680	9360	96.7%	948	584	61.6%	Commerce Learning Management System (Karta) and other commercial training sources.	$505,659

G.2.

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes

Comments: (G.1.a--G.1.b) Responses are based on evidence from a sample of operating units within Census, NIST, and NOAA, and all units of USPTO. We obtained data bases identifying awareness training taken by employees, but did not validate whether the total number of employees identified as needing training was correct.

(G.1.c--G1.d) Responses are based on evidence from all of Census, NIST, USPTO, and one unit of NOAA. We obtained data bases identifying specialized training taken by employees, but did not validate whether the total number of employees with significant IT security responsibilities was correct.

(G.2) Department awareness training explains peer-to-peer file sharing; however, not all of the awareness training provided by the Department's bureaus address this topic.