OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

Federal Information Security Management Act

Fiscal Year 2004 Status of EPA's Computer Security Program

Report No. 2004-S-00007

September 30, 2004

Report Contributors:

Ed Densmore
Anita Mooney
Vincent Campbell
Cheryl Reid

Abbreviations

EPA	Environmental Protection Agency
C&A	Certification and Accreditation
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IFMS	Integrated Financial Management System
IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

September 30, 2004

MEMORANDUM

SUBJECT: Federal Information Security Management Act:
Fiscal Year 2004 Status of EPA's Computer Security Program
Report No. 2004-S-00007

TO: Michael O. Leavitt
Administrator

Attached is our final report entitled *Federal Information Security Management Act: Fiscal Year 2004 Status of EPA's Computer Security Program.* This report synopsizes the results of information technology security work the U.S. Environmental Protection Agency's Office of Inspector General (OIG) performed during Fiscal Year (FY) 2004. This report includes the OIG's completed FY 2004 FISMA Reporting Template, as prescribed by the Office of Management and Budget (OMB).

In accordance with OMB reporting instructions, I am forwarding this report to you for submission, along with the Agency's required information, to the Director, OMB.

Nikki L. Tinsley /s/

Attachment

cc:
K. Nelson, Assistant Administrator for Environmental Information (OEI) (2810A)
M. Day, Director, Office of Technology Operations and Planning (OTOP) (2831T)
G. Bonina, Senior Agency Information Security Officer (2831T)
R. Gonzalez, Director, National Technology Services Division (NTSD) (N229-01)
M. Cody, Associate Director, Technical Information Security Staff (TISS) (2831T)
J. Gibson, Operations Security Manager, NTSD (N276-01)
J. Worthington, OEI Audit Coordinator (2812T)
R. Trent, OEI Audit Coordinator (2831T)
K. Farmer, TISS Audit Coordinator (2831T)

Fiscal Year 2004 Status of EPA's Computer Security Program

The Federal Information Security Management Act (FISMA) requires the Office of Inspector General (OIG) to perform an independent evaluation of the Agency's information security program and practices. We performed our work in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. The following summarizes information security work we performed during fiscal 2004.

Information Technology Security Performance

In general, Agency officials have taken positive actions to secure EPA's information resources. EPA has adequate physical security controls to protect its network firewalls, including comprehensive continuity of operations plans. However, our audit entitled *EPA's Administration of Network Firewalls Needs Improvement*, Report Number 2004-P-00013, dated March 31, 2004, disclosed logical and configuration control weaknesses which need to be improved to further secure information resources. We recommended several actions to the Director, Office of Technology, Operations, and Planning, to improve EPA's firewall security, including: establishing a standard configuration requirement for adequately securing workstations used to remotely administer the network firewalls; modifying the change and patch management processes to ensure that when firewall changes and patches are applied they do not adversely affect previously applied fixes; and modifying the network vulnerability assessment methodology to include scanning of all firewall components. Agency officials concurred with our recommendations and reported that corrective actions were to be implemented by September 30, 2004.

We also evaluated the adequacy of policies, procedures, and practices for controlling financial application development and software changes to EPA's Integrated Financial Management System (IFMS). Our audit entitled *EPA Needs to Improve Change Controls for Integrated Financial Management System*, Report Number 2004-P-00026, dated August 24, 2004, reported a general breakdown of security controls that could undermine the integrity of IFMS software libraries and financial system data. Duties had not been adequately segregated, individuals used an inappropriate ID or continued to have system access after no longer needing it, and contractor personnel were granted access to IFMS without a successful background security check. Further, management had not instituted a formal, structured change control process for IFMS to ensure software program modifications were properly authorized, tested, and approved. We made various recommendations to the Chief Financial Officer and the Acting Assistant Administrator for Administration and Resources Management to improve IFMS controls and institutionalize security screening procedures. In commenting on the draft report, the Chief Financial Officer concurred with our recommendations and generally outlined appropriate corrective actions to improve security and change controls over IFMS. The Acting Assistant Administrator for Administration and Resources Management did not concur with our recommendations concerning contractor background investigations, asserting that "suitability" background investigations of Federal contractors are not required. Management stated its existing, interim procedures were sufficient to guide offices that chose to initiate background

investigations. However, current EPA policy and Federal guidance strongly recommend screening comparable to that for Federal staff, and we strongly urge such screening. A response to the final report is due by November 24, 2004.

Plan of Action and Milestones

EPA has developed, implemented, and is managing an adequate, Agency-wide plan of action and milestones (POA&M) process. We reviewed EPA's POA&M process, which included validating a sample of "completed" POA&Ms from the Agency's December 2003 Quarterly Report to the Office of Management and Budget. Our validation methodology included reviewing supporting documentation and interviewing appropriate personnel to determine if the corrective actions taken adequately addressed the weakness and complied with applicable Federal criteria.

In general, EPA's POA&M process incorporates known Information Technology (IT) security weaknesses, developed by both program officials and the Chief Information Officer. The Chief Information Officer centrally tracks, maintains, and reviews POA&M activities. We found the POA&M process does not currently prioritize security weaknesses; however Agency officials are actively addressing this issue and expect to complete the first phase of a two-phased prioritization development process by November 2004. We also identified some errors with the data, but we did not consider them to be of a "material" nature and concluded that (1) most of the inaccuracies stemmed from the newness of the tracking system and (2) these problems would be rectified as soon as OEI issued additional administrative guidance. We made suggestions to improve the quality of the data, and Agency officials discussed our concerns at the 2004 Information Security Officer training conference.

Certification and Accreditation

The Agency's Certification and Accreditation (C&A) process complies with Federal guidance. In assessing the Agency's C&A process, we used the Government Accountability Office's (GAO) report entitled *Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation,* Report Number GAO-04-376, dated June 2004. In a survey of 24 major departments and agencies, GAO found that agencies need to implement consistent processes in authorizing systems for operation. Based on its field work of six systems, GAO prepared a statement of facts summarizing findings specific to EPA and indicated that the Agency's C&A process and specific C&A packages generally complied with Federal C&A criteria. However, GAO indicated that they found varying degrees of comprehensiveness at EPA and instances where required steps were incomplete, such as missing and/or untested contingency plans and missing risk assessments. In addition, although EPA's system self-assessments stated that security controls had been "tested," GAO found limited documentation to support that these controls had actually been tested on an annual basis. The only evidence GAO found was the results of technical vulnerability assessments, which were conducted as part of periodic risk assessments. Further, in some cases, GAO found it difficult to determine the actual risk being accepted by EPA in the accreditation decision.

Incident Detection and Handling

The Agency's incident detection and handling practices comply with documented policies and procedures. We reviewed the Agency's processes for incident handling by examining a sample of security incidents taken from the Computer Security Incident Response Center's weekly reports. We tracked these incidents through the process to determine how they were identified, remedied, and reported internally, as well as externally, if applicable. We found the Agency followed defined policies and procedures for reporting incidents internally, as well as externally to law enforcement and the US Computer Emergency Readiness Team.

Security Training and Awareness

EPA continues to make improvements in providing and recording training to ensure security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities. For example, EPA indicated that 49 percent of personnel with significant IT responsibilities received training in fiscal 2004, up from 31 percent in fiscal 2003. During this past year, the Agency implemented an on-line IT Security training library available through the Federal government's E-learning portal (i.e., GoLearn.gov). The GoLearn.gov IT security library contains 13 role-based training plans. Agency officials identified employees with significant security responsibilities by 1 of the 13 functional roles, and pre-registered these employees into the Go-Learn training system. In addition, it was recommended these employees take at least two of the Go-Learn courses by August 31, 2004.

2004 FISMA Report

Agency:	Environmental Protection Agency
Date Submitted:	10/6/2004
Submitted By:	OIG

Contact Information:

Name:	Pat Hill
E-mail:	Hill.Pat@EPA.gov
Phone:	202-566-0894

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.

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
Office of the Administrator	1	0	2		0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Office of Air and Radiation	1	0	19	2	2	0		0.0%	2	10.5%		0.0%	0	0.0%	0	0.0%
Office of Administration and Resources Management	1	0	12	4	2	0	1	8.3%	3	25.0%	1	8.3%		0.0%		0.0%
Office of the Chief Financial Officer	1	0	18	12	0	0		0.0%	2	11.1%	10	55.6%		0.0%		0.0%
Office of Enforcement and Compliance	1	0	11	2	0	0		0.0%	2	18.2%		0.0%		0.0%		0.0%
Office of Environmental Information - Central	2	0	38	16	1	0	3	7.9%	11	28.9%	3	7.9%		0.0%		0.0%
Office of Environmental Information - Non Central*		0			7											
Office of General Counsel	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Office of International Activities	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Office of Inspector General	1	0	9	9	0	0	9	100.0%	9	100.0%	8	88.9%	9	100.0%	9	100.0%
Office of Prevention, Pesticides, and Toxic Substances	1	0	9	2	0	0	1	11.1%	1	11.1%	1	11.1%		0.0%		0.0%
Office of Research and Development	1	0	16	1	0	0		0.0%		0.0%		0.0%	1	6.3%	1	6.3%
Office of Solid Waster and Emergency Response	1	0	13	3	7	0		0.0%	3	23.1%		0.0%	1	7.7%	0	0.0%
Office of Water	1	0	10	3	0	0		0.0%	2	20.0%	1	10.0%		0.0%		0.0%
Region 1 - Boston	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 2 - New York	1	0	1	1	0	0		**0.0%**		0.0%		0.0%	1	100.0%	1	100.0%
Region 3 - Philadelphia	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 4 - Atlanta	1	0	1	1	0	0	1	100.0%		0.0%		0.0%		0.0%		0.0%
Region 5 - Chicago	1	0	3	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 6 - Dallas	1	0	2	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 7 - Kansas City	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 8 - Denver	1	0	2	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 9 - San Francisco	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Region 10 - Seattle	1	0	1	0	0	0		0.0%		0.0%		0.0%		0.0%		0.0%
Agency Total	**24**	**0**	**173**	**56**	**19**	**0**	**15**	**8.7%**	**35**	**20.2%**	**24**	**13.9%**	**12**	**6.9%**	**11**	**6.4%**

Comments: * The OIG did not differentiate between OEI-Central and OEI-Non-Central programs and, therefore, reported all systems reviewed under OEI-Central.

A.1.b. - The OIG did not use NIST 800-26 in its entirety for these reviews.

A.2 - The universe of systems reviewed for A.2.a. through A.2.e. represents unique subsets of the Agency total of 173; based on individual reviews conducted by GAO or the OIG. The universe for A.2.a.through A.2.e. is 15, 35, 24, 13 and 13 respectively.

This page reflects the OIG response, which differs from the Agency Response. Per OMB requirements, the Agency response has been submitted under separate cover.

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.	Almost Always, or 96-100% 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.	
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.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% 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.c. is actually "Not Applicable" since the NIST self-assessment guide was used to conduct all system reviews.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.

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
			For FY04, EPA did not have any significant deficiencies in policies, procedures, or practices to report.	
Agency Total	0	0		

Comments:

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.

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.	Almost Always, or 96-100% 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.	Almost Always, or 96-100% 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.	Rarely, or 0-50% of the time

Comments:
C.1.j. - The Agency has begun a process to prioritize POA&Ms. They are currently assigning and assessing risk values for the NIST 800-26 questions. The Agency expects to complete this phase by November 2004. In the next phase, the Agency plans to apply a cost estimate to the risks, with a planned completion of May 2005.

C.1 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: In assessing the Agency's Certification and Accreditation (C&A) process, we used audit work performed by the Government Accountability Office (GAO). In a statement of facts summarizing GAO's C&A review at EPA, GAO indicated that the Agency's C&A process and specific C&A packages generally complied with C&A criteria found in federal guidance. However, GAO also indicated that they found varying degrees of comprehensiveness and instances where required steps were incomplete, such as missing and/or untested contingency plans, and missing risk assessments. In addition, although EPA's system self-assessments stated that security controls had been "tested," GAO found limited documentation to support that these controls had actually been tested on an annual basis. The only available evidence GAO could find was the results of technical vulnerability assessments, which were conducted as part of periodic risk assessments. Further, in some cases GAO found it difficult to determine the actual residual risk being accepted in the accreditation decision. Based on GAO's findings, we find EPA's C&A process to be satisfactory.	Satisfactory

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.

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 agency-wide 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 agency-wide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?		
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	Yes	Almost Always, or 96-100% of the time
d. Windows 2000	Yes	Rarely, or 0-50% of the time
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	Yes	Almost Always, or 96-100% of the time
g. Solaris	Yes	Almost Always, or 96-100% of the time
h. HP-UX	Yes	
i. Linux	Yes	Almost Always, or 96-100% of the time
j. Cisco Router IOS	No	
k. Oracle	Yes	Rarely, or 0-50% of the time
l. Other. Specify: Netware, HP Tru 64, IBM AIX, and SGI IRIX	Yes	Almost Always, or 96-100% of the time
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Almost Always, or 96-100% of the time

Comments: D.1 - Agency officials compiled the evaluation responses in late September 2004, and therefore, the OIG did not independently verify them.
D.1.h. - The Agency did not evaluate this configuration because it is no longer used in the Agency.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.

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.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% 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	Almost Always, or 96-100% 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?	95	55%

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

Answer:

The OIG and Agency use Symantec NetRecon, NESSUS, and Internet Security Systems to conduct technical vulnerability assessments. The Agency Tools also include NMap, TNT, EtherPeek, and PatchLink. Technical controls are firewalls, IDSs, perimeter controls, configuration management, and CSIRC and vulnerability management solutions.

Comments:

E.1. - The OIG used a sample to evaluate the Agency's compliance with defined policies and procedures for reporting incidents internally and externally to law enforcement authorities and to US-CERT.

E.2.a. - This number reflects scans performed by the OIG as well as the Agency. The OIG performed a variety of scans on 13 systems.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.

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	0	0	0	0	0	0
II. User Compromise	0	0	0	0	0	0
III. Denial of Service Attack	1	1	0	1	0	0
IV. Website Defacement	0	0	0	0	0	0
V. Detection of Malicious Logic	1	1	0	1	0	0
VI. Successful Virus/worm Introduction	224	224	1	63	2	12
VII. Other	29	29	3	3	0	0
Totals:	255	255	4	68	2	12

Comments:

Agency officials compiled this data in late September 2004, and therefore, the OIG did not independently verify the data. However, during the OIG review of the Agency's incident handling process, we did not find evidence contradicting the Agency response.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.

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		
23,404	21,024	90%	821	406	49%	GoLearn and Other Training (See Comments for brief description)	$476,802

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?	No

Comments:
Agency officials compiled this data in late September 2004, and therefore, the OIG did not independently verify the data. However, during the OIG review of the Agency's training process, we did not find evidence contradicting the Agency response.

G.1.e. - Government Online Learning Center's (GoLearn) IT Security Training Library, composed of more than 75 IT security-related courses in Data Security, Network Security, Security Planning and Security Policy/Guidelines; National Defense University provides training in Information Resource Management; and the EPA's 2004 IT Security and Operations Conference in Research Triangle Park, included (but not all inclusive) training modules in Anytime Anyplace Access, Risk Assessments, Security Plans, Certification and Accreditation, Wireless LAN, Patch Management, Contingency Planning, Incident Response, and Bindview.