OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Federal Information Security Management Act

Fiscal Year 2005 Status of EPA's Computer Security Program

Report No. 2006-S-00001

October 3, 2005

Report Contributors:

Rudolph M. Brevard
Charles Dade
Cheryl Reid
Neven Morcos
Sejal Shah

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

INSPECTOR GENERAL

October 3, 2005

MEMORANDUM

SUBJECT: Fiscal Year 2005 Federal Information Security Management Act Report

TO: Stephen L. Johnson
Administrator

Attached is the Office of Inspector General's (OIG) completed Fiscal Year (FY) 2005 Federal Information Security Management Act Reporting Template, as prescribed by the Office of Management and Budget (OMB). In addition, Appendix A synopsizes the results of our significant FY 2005 information security audits.

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, Office of Management and Budget.

for Rudolph M Brevard
Nikki L. Tinsley

Attachment

cc:
Assistant Administrator for Environmental Information and Chief Information Officer
Director, Office of Technology Operations and Planning
Senior Agency Information Security Officer
Director, National Technology Services Division
Associate Director, Technical Information Security Staff
Operations Security Manager, National Technology Services Division
Audit Coordinator, Office of Environmental Information
Audit Coordinator, Technical Information Security Staff

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Environmental Protection Agency

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						**Question 2**					
		a. FY 05 Agency Systems		**b. FY 05 Contractor Systems**		**c. FY 05 Total Number of Systems**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Office of Administrator	High	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Air and Radiation		2	1	0	0	2	1	0	0.0%	1	100.0%	1	100.0%
	Moderate	11	0	0	0	11	0			0	0.0%	0	0
	Low	4	0	2	0	6	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**17**	**1**	**2**	**0**	**19**	**1**	**0**	**0.0%**	**1**	**100.0%**	**1**	**100.0%**

High

		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Office of Administration and Resources Management	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	6	1	2	0	8	1	0	0.0%	1	100.0%	0	0.0%
	Low	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**9**	**1**	**2**	**0**	**11**	**1**	**0**	**0.0%**	**1**	**100.0%**	**0**	**0.0%**
Office of Chief Financial Officer	High	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	16	7	0	0	16	7	0	0.0%	0	0.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**18**	**7**	**0**	**0**	**18**	**7**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Enforcement and Compliance Assurance	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	1	0	0	8	1	0	0.0%	1	100.0%	0	0.0%
	Low	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**10**	**1**	**0**	**0**	**10**	**1**	**0**	**0.0%**	**1**	**100.0%**	**0**	**0.0%**
Office of Environmental Information-Central	High	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	6	1	1	0	7	1	0	0.0%	1	100.0%	0	0.0%
	Low	4	0	0	0	4	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**13**	**1**	**1**	**0**	**14**	**1**	**0**	**0.0%**	**1**	**100.0%**	**0**	**0.0%**
Office of Environmental Information-Non-Central	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	10	0	3	0	13	0	0	0.0%	0	0.0%	0	0.0%
	Low	8	0	3	0	11	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized		0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**18**	**0**	**6**	**0**	**24**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**

		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Office of General Counsel	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low		0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of International Activities	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of the Inspector General	High	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Low	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**8**	**0**	**0**	**0**	**8**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Prevention Pesticides and Toxic Substances	High	0	0	0	0	0	0	0	0.0%	0	0.0%		0.0%
	Moderate	6	0	0	0	6	0	0	0.0%	0	0.0%	0	0.0%
	Low	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**8**	**0**	**0**	**0**	**8**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Research and Development	High	5	0	0	0	5	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	6	0	0	0	6	0	0	0.0%	0	0.0%	0	0.0%
	Low	3	0	0	0	3	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**14**	**0**	**0**	**0**	**14**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**

		a. FY 05 Agency Systems		**b. FY 05 Contractor Systems**		**c. FY 05 Total Number of Systems**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Office of Solid Waste and Emergency Response	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	6	1	0	0	6	1	0	0.0%	1	100.0%	0	0.0%
	Low	5		1	0	6	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**11**	**1**	**1**	**0**	**12**	**1**	**0**	**0.0%**	**1**	**100.0%**	**0**	**0.0%**
Office of Water	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	9	1	0	0	9	1	0	0.0%	1	100.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**10**	**1**	**0**	**0**	**10**	**1**	**0**	0.0%	**1**	100%	**0**	**0.0%**
Region 1	High		0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low		0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 2	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 3	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**

		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Region 4	High	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 5	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	2	0	0	0	2	0	0	0.0%	0	0.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 6	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 7	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 8	High	0	0	0	0	0	0	0	0.0%		0.0%		0.0%
	Moderate	1	0	0	0	1	0	0	0.0%		0.0%		0.0%
	Low	1	0	0	0	1	0	0	0.0%		0.0%		0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**

		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	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
Region 9	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 10	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Low	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Sub-total	**155**	**13**	**12**	**0**	**167**	**13**	**0**	**0.0%**	**6**	**100.0%**	**1**	**20.0%**
Agency Totals	**High**	**16**	**1**	**0**	**0**	**16**	**1**	**0**	**0.0%**	**1**	**16.7%**	**1**	**20.0%**
	Moderate	**100**	**12**	**6**	**0**	**106**	**12**	**0**	**0.0%**	**5**	**83.3%**	**0**	**0.0%**
	Low	**39**	**0**	**6**	**0**	**45**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Total	**155**	**13**	**12**	**0**	**167**	**13**	**0**	**0.0%**	**6**	**100.0%**	**1**	**20.0%**

Comments: Question 1- The OIG accepted the Agency's numbers as accurate without verification. Question 2 The universe of systems reviewed for 2.a through 2.c represents unique subsets of the Agency's systems, based on individual reviews conducted by the OIG. The universes for: 2.a is 7; 2.b is 6; and 2.c is 5. Therefore, we calculated the respective column percentages by dividing the respective number by the universe for that column. 2.b we gave credit for system testing and evaluations if the security of the servers associated with the systems were being monitored using vulnerability scanning software (such as ISS or Nessus) or configuration management software (such as Bindview or ESM).

	Question 3	
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: Rarely, for example, approximately 0-50% of the time Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Almost Always, for example, approximately 96-100% of the time
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: Approximately 0-50% complete Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.c.	The OIG **<u>generally</u>** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **<u>generally</u>** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes
Comment: 3.c and 3.d - The OIG accepted the Agency's numbers as accurate without verification.		

[redacted]

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. 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 area provided below.

For items 4a.-4.f, the response categories are as follows:

Rarely, for example, approximately 0-50% of the time
Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time
-

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Almost Always, for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)	Almost Always, for example, approximately 96-100% of the time .
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	Almost Always, for example, approximately 96-100% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	Almost Always, for example, approximately 96-100% of the time

discover security weaknesses that should have been easily identified.

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "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 .

Assess the overall quality of the Department's certification and accreditation process.

Response Categories:

- Excellent
- Good
- Satisfactory
- Poor
- Failing

- Good

Comments: This is based on auditor opinion that EPA's overall rating for C&A existing policies are excellent (OMB response category), oversight and review processes are good (OMB response category), and Program Office execution (for our five selected systems) is poor (OMB response category).

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name: Environmental Protection Agency

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	
HP-UX	N/A	No	
Linux	Yes	Yes	
Cisco Router IOS	Yes	Yes	
Oracle	Yes	Yes	
Other. Specify: Unix 5.1	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software

Comments: We reviewed a small subset of server configuration settings on a total of 4 servers (1 for each of 4 of the product's configuration settings we commented on above). We had the following results: Windows 2000 Server, we reviewed 17 out of 134 settings included in the SCD and found 15 complied. For Windows 2003 Server, we reviewed 17 out of 183 settings included in the SCD and found 17 complied. For Windows NT, we reviewed 10 out of 101 settings included in the SCD and found 10 complied. For Unix 5.1, we reviewed 7 out of 89 settings included in the SCD and found 6 complied.

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		

Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Comment:		

Question 9		
9	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 or No.	Yes

Summary of Significant Fiscal 2005 Security Control Audits

During Fiscal 2005, EPA's Office of Inspector General (OIG) conducted several audits of EPA's information technology security program and information systems. The following summary synopsizes key findings and recommendations. Copies of all final reports are located on the OIG's Internet site at *http://www.epa.gov/oig/publications.htm.*

1. Audit of EPA's Fiscal 2004 and 2003 Financial Statements, Report No. 2005-1-00021, November 15, 2004

The requirement for audited financial statements was enacted to help bring about improvements in agencies' financial management practices, systems, and controls so that timely and reliable information is available for managing Federal programs. In conjunction with this audit, we reported Reportable Conditions related to system development, and certification and accreditation, of EPA's Grant Payment Allocation System (GPAS) and Inter-Governmental Document Online Tracking System (IDOTS). In addition, we continued to report that we are unable to assess the application processing controls surrounding the Integrated Financial Management System (IFMS) – EPA's core financial system. Specifically, we reported:

- The Office of Chief Financial Officer (OCFO) developed and implemented the GPAS and IDOTS accounting systems without assessing the risks these systems pose to Agency assets, personnel, and operations. In addition, EPA did not produce key security documents for these systems, nor ensure management controls were operating effectively by assessing and testing security controls for the GPAS and IDOTS. We made several recommendations to OCFO's Director, Office of Financial Services to improve the GPAS and IDOTS' security. These included: (1) conducting a formal risk assessment; (2) conducting a review of GPAS' compliance with all applicable Joint Financial Management Improvement Program system requirements; and (3) directing offices to follow Agency system development policy. We also, recommended that the Director: (1) complete and document a formal certification and accreditation; (2) update the systems' certification and accreditation status in the Agency's self-assessment database; (3) develop and implement a formal patch management process; and (4) implement a formal process to conduct vulnerability scanning and control testing on a regular basis.

- We continue to be unable to assess the adequacy of the automated application control structure as it relates to automated input, processing, and output controls for IFMS. Since IFMS has a direct and material impact on the Agency's financial statements, assessing each application is necessary to determine the reliance we can place on the financial statements. During past financial statement audits, we attempted to evaluate controls without systems documentation, but these alternatives proved to be inefficient and impractical. OCFO has no plans to update the IFMS system documentation until it implements the new financial replacement software package, currently projected for Fiscal 2008. Until the new system is in place, we cannot assess the adequacy of the automated internal control structure.

2. Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement, Report No. 2005-P-00011, March 22, 2005

Our audit of various EPA remote access methodologies determined that system administrators did not configure Web-Mail and BlackBerry servers to provide secure remote access to the Agency's network. We found that the system administrators did not configure or update 59 percent of the Web-Mail and BlackBerry servers to mitigate vulnerabilities. We also found several of the Agency's BlackBerry devices were not adequately configured, secured, or monitored. We found deficiencies in security configuration settings and physical security of BlackBerry devices.

We made several recommendations to EPA's Director, Office of Technology Operations and Planning. These included establishing and requiring all remote access systems to have security monitoring and network vulnerability scanning; developing standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System; and conducting a risk assessment and establishing a process to consistently configure devices. The Agency generally agreed with the recommendations and indicated corrective actions that, when implemented, would address the recommendations.

3. PeoplePlus Security Controls Need Improvement, Report No. 2005-P-00019, July 28, 2005

Our review identified three significant issues in the security administration of PeoplePlus. First, the Agency had not followed prescribed procedures for managing user access privileges, monitoring changes in employee responsibilities, and processing system access requests. Second, EPA did not verify or conduct the required National Agency Check with Inquiries and Credit background screenings for 45 percent (10 of 22) of contractor personnel with PeoplePlus access. Third, EPA implemented PeoplePlus without adequately implementing security controls for two key processes. Specifically, the Office of Chief Financial Officer had not properly secured default user IDs and did not adequately separate incompatible duties performed by the Security Administrator.

We recommended the Directors of EPA's Office of Financial Services and Office of Human Resources take 13 actions to improve PeoplePlus security controls. These recommendations address areas where EPA could improve user access management and contractor background screening procedures. These recommendations include: (1) reinforcing the requirements to follow prescribed policies and procedures; (2) providing a training program to increase awareness and ability to perform security duties; (3) evaluating the need for system development contractors to have access to the production environment; and (4) establishing a milestone date to complete contractor background screening. We recommended that EPA evaluate all default user IDs to secure them, and assign Security Administrators' responsibilities in a manner that provides adequate separation of incompatible duties. EPA concurred with all of our recommendations and provided a plan of action to address concerns.

4. Agency Information Systems Security Controls Audit, Planned Final Report Date is October 2005

Our objectives were to provide an independent evaluation of the information security program and practices of the Agency. This included selecting a sample of EPA's information systems and: (1) evaluating certification and accreditation to determine Agency compliance with Federal guidance; (2) determining whether security control costs are integrated into the life cycle of the system; (3) determining whether security controls have been tested and evaluated in the last year; (4) reviewing contingency plans and the testing of plans; (5) reviewing compliance with system standard configuration documents; and (6) conducting and analyzing results of technical vulnerability scans. We began this audit in February 2005 and plan to issue the final report in October 2005.

5. Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at the Research Triangle Park Campus, Planned Final Report Date is November 2005

The OIG hired a contractor to access physical assess controls and service continuity/contingency for financial and mixed-financial applications located at its Research Triangle Park Campus in North Carolina. The audit's objectives were to: (1) gather the inventory of financial and mixed financial applications hosted at the Research Triangle Park facility to guide their review; (2) evaluate physical security controls in accordance with relevant Federal and EPA criteria and best practices; and (3) evaluate service continuity/contingency controls in accordance with relevant Federal and EPA criteria and best practices. The contractor began this audit in February 2005 and plans to issue its final report in November 2005.