U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Fiscal Year 2008 Federal Information Security Management Act Report

Status of EPA's Computer Security Program

Report No. 08-P-0280

September 26, 2008

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

OFFICE OF
INSPECTOR GENERAL

September 26, 2008

MEMORANDUM

SUBJECT: Fiscal Year 2008 Federal Information
Security Management Act Report:
Status of EPA's Computer Security Program
Report No. 08-P-

Patricia H. Hill

FROM: Patricia H. Hill
Assistant Inspector General for Mission Systems

TO: Stephen L. Johnson
Administrator

Attached is the Office of Inspector General's Fiscal Year 2008 Federal Information Security Management Act Reporting Template, as prescribed by the Office of Management and Budget. This audit was performed by Williams, Adley and Company, LLP, under the direction of the U.S. Environmental Protection Agency's Office of Inspector General. In addition, Appendix A synopsizes the results of our significant Fiscal Year 2008 information security audits.

The estimated cost for performing this audit, which includes contract costs and Office of Inspector General contract management oversight, is $388,135.

In accordance with Office of Management and Budget 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.

Section C - Inspector General: Questions 1 and 2

Agency Name:	**Environmental Protection Agency**	**Submission date:**	**September 25, 2008**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2.   For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						**Question 2**					
		a. Agency Systems		**b. Contractor Systems**		**c. Total Number of Systems (Agency and Contractor systems)**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and reviewed in the past year**		**c. Number of systems for which contingency plans have been tested in accordance with policy**	
U.S. Environmental Protection Agency	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
OA	High	0	0	0	0	0	0	0		0		0	
	Moderate	2	0	0	0	2	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**		**0**		**0**	
OAR	High	1	0	0	0	1	0	0		0		0	
	Moderate	11	1	1	0	12	1	1	100%	0	0%	1	100%
	Low	6	0	1	0	7	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**18**	**1**	**2**	**0**	**20**	**1**	**1**	100%	**0**	0%	**1**	100%
OARM	High	0	0	0	0	0	0	0		0		0	
	Moderate	11	0	2	1	13	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**11**	**0**	**2**	**1**	**13**	**1**	**1**	100%	**1**	100%	**1**	100%
OCFO	High	0	0	0	0	0	0	0		0		0	
	Moderate	18	1	0	0	18	1	1	100%	1	100%	1	100%
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**19**	**1**	**0**	**0**	**19**	**1**	**1**	100%	**1**	100%	**1**	100%
OECA	High	0	0	0	0	0	0	0		0		0	
	Moderate	8	1	0	0	8	1	1	100%	1	100%	1	100%
	Low	3	1	0	0	3	1	1	100%	0	0%	1	100%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**11**	**2**	**0**	**0**	**11**	**2**	**2**	100%	**1**	50%	**2**	100%
OEI	High	0	0	0	0	0	0	0		0		0	
	Moderate	16	0	6	1	22	1	1	100%		0%	1	100%
	Low	16	1	3	0	19	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**32**	**1**	**9**	**1**	**41**	**2**	**2**	100%	**1**	50%	**2**	100%
OGC	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	

Section C - Inspector General: Questions 1 and 2

Agency Name:	**Environmental Protection Agency**
Submission date:	**September 25, 2008**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						**Question 2**					
		a. **Agency Systems**		**b.** **Contractor Systems**		**c.** **Total Number of Systems (Agency and Contractor systems)**		**a.** **Number of systems certified and accredited**		**b.** **Number of systems for which security controls have been tested and reviewed in the past year**		**c.** **Number of systems for which contingency plans have been tested in accordance with policy**	
U.S. Environmental Protection Agency	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
OIA	High	0	0	0	0	0	0	0		0		0	
	Moderate	0	0	0	0	0	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
OIG	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	0	0	0	7	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**7**	**0**	**0**	**0**	**7**	**0**	**0**		**0**		**0**	
OPPTS	High	0	0	0	0	0	0	0		0		0	
	Moderate	6	1	1	0	7	1	1	100%	1	100%	1	100%
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**7**	**1**	**1**	**0**	**8**	**1**	**1**	100%	**1**	100%	**1**	100%
ORD	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	0	0	0	7	0	0		0		0	
	Low	8	0	0	0	8	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**15**	**0**	**0**	**0**	**15**	**0**	**0**		**0**		**0**	
OSWER	High	0	0	0	0	0	0	0		0		0	
	Moderate	4	1	1	0	5	1	1	100%	1	100%	1	100%
	Low	4	0	1	0	5	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**8**	**1**	**2**	**0**	**10**	**1**	**1**	100%	**1**	100%	**1**	100%
OW	High	0	0	0	0	0	0	0		0		0	
	Moderate	8	0	0	0	8	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**8**	**0**	**0**	**0**	**8**	**0**	**0**		**0**		**0**	
R01	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	1	0	0	1	1	1	100%	0	0%	1	100%
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**0**	0%	**1**	100%

Section C - Inspector General: Questions 1 and 2

Agency Name:	**Environmental Protection Agency**	**Submission date:**	**September 25, 2008**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						**Question 2**					
		a. Agency Systems		**b. Contractor Systems**		**c. Total Number of Systems (Agency and Contractor systems)**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and reviewed in the past year**		**c. Number of systems for which contingency plans have been tested in accordance with policy**	
U.S. Environmental Protection Agency	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
R02	High	0	0	0	0	0	0	0		0		0	
	Moderate	2	0	0	0	2	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**		**0**		**0**	
R03	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
R04	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
R05	High	0	0	0	0	0	0	0		0		0	
	Moderate	2	0	0	0	2	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**		**0**		**0**	
R06	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
R07	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
R08	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	0	0	1	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**		**0**		**0**	

Section C - Inspector General: Questions 1 and 2

Agency Name:	Environmental Protection Agency	Submission date:	September 25, 2008

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						**Question 2**					
		a. **Agency Systems**		**b.** **Contractor Systems**		**c.** **Total Number of Systems (Agency and Contractor systems)**		**a.** **Number of systems certified and accredited**		**b.** **Number of systems for which security controls have been tested and reviewed in the past year**		**c.** **Number of systems for which contingency plans have been tested in accordance with policy**	
U.S. Environmental Protection Agency	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
R09	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	0	1	0	2	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**1**	**0**	**2**	**0**	**0**		**0**		**0**	
R10	High	0	0	0	0	0	0	0		0		0	
	Moderate	0	0	0	0	0	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
	Moderate	**110**	**6**	**12**	**2**	**122**	**8**	**8**	100%	**5**	63%	**8**	100%
	Low	**43**	**2**	**5**	**0**	**48**	**2**	**2**	100%	**1**	50%	**2**	100%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**154**	**8**	**17**	**2**	**171**	**10**	**10**	100%	**6**	60%	**10**	100%

🟨	= Data Entry Cells
⬜	= Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

Section C - Inspector General: Question 3

Agency Name: **Environmental Protection Agency**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of 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.** 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. 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	Mostly (81-95% of the time)
3.b.	**The agency has developed a complete 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: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally 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 or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes

3.f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits}	Agency or Contractor system?

Number of known systems missing from inventory:	0

🟨 = Data Entry Cells

Section C - Inspector General: Questions 4 and 5

Agency Name:	**Environmental Protection Agency**

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

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**

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 (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 (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (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 (96-100% of the time)
POA&M process comments:	EPA has developed and implemented a POA&M program that ensures CIO reports on a regular basis the security weaknesses and remediation at least quarterly. The processes and procedures ensures OEI tracks, maintains, and reviews POA&M activities on a quarterly basis for weaknesses reported by EPA.	

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good

5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	
		Security control testing	X
		Incident handling	
		Security awareness training	
		Configurations/patching	
		Other:	

C&A process comments:	From our sample of 10 systems all had C&A documents. However 4 out of 10 did not provide security test results.

Section C - Inspector General: Questions 6, 7, and 8

Agency Name:	**Environmental Protection Agency**	
Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
Comments:		
7	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
Comments:	EPA is in the process of implementing program. Policies have been drafted. Procedures have been developed and implemented. Training is being provided.	
Question 8: Configuration Management		
8.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
Comments:		
8.b.	**Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.** **Response categories:**	Mostly (81-95% of the time)
	- 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	
Comments:	EPA should take additional steps to ensure that network configurations are maintained. Our tests disclosed security patches and updates on network resouces were not always timely installed.	
8.c.	**Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:**	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section C - Inspector General: Questions 9, 10 and 11

Agency Name:	Environmental Protection Agency	
Question 9: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	Yes
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:		
Question 10: Security Awareness Training		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees		Almost Always (96-100% of employees)
Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing		
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.		Yes
Question 12: E-Authentication Risk Assessments		
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, “Electronic Authentication Guidelines”? Yes or No.		Yes
12.b. If the response is “No”, then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.		

Appendix A

Summary of Significant Fiscal Year 2008 Security Control Audits

During Fiscal Year 2008, the U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) initiated the following audits of EPA's information technology security program and information systems. The following synopsizes key findings.

1. Supplemental Fiscal 2007 FISMA Audit Results: OIG Results of EPA's Efforts to Protect PII and Contractor Results of EPA Standard Configuration Documents' Compliance with Federal Guidance or Industry Best Practices Assignment No. 2007-000802, December 20, 2007

EPA needs to (1) issue a memo to Senior Information Officers to remind them of the Agency's policy requirements for protecting personally identifiable information and the need to reiterate and reinforce compliance with the Agency policy, and (2) complete efforts to publish the Privacy Program procedures related to the Privacy Program policy.

EPA concurred with the recommendations and subsequently implemented corrective actions to adequately address the report recommendations.

2. Review of the Quality of Self-Reported Security Information in EPA's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) System, Assignment No. 2008-0003

The primary objective of this assignment is to determine whether EPA has implemented effective management control processes for maintaining the quality of the data in EPA's ASSERT system. The OIG plans to issue a final report by December 2008.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Director, Office of Technology Operations and Planning, Office of Environmental Information
Senior Agency Information Security Officer, Office of Environmental Information
Agency Follow-up Official (the CFO)
Agency Follow-up Coordinator
Office of General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Deputy Inspector General