OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Fiscal Year 2007 Federal Information Security Management Act Report

Status of EPA's Computer Security Program

Report No. 2007-S-00003

September 25, 2007

Report Contributors: Rudolph M. Brevard
Vincent Campbell
Sejal Shah
Sabrena Stewart

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

OFFICE OF
INSPECTOR GENERAL

September 25, 2007

MEMORANDUM

SUBJECT: Fiscal Year 2007 Federal Information Security Management Act Report: Status of EPA's Computer Security Program
Report No. 2007-S-00003

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 2007 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 Fiscal Year 2007 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.

Section C - Inspector General: Questions 1 and 2

Agency Name: Environmental Protection Agency **Submission date:** 21-Sep-07

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	
Bureau Name	**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
Office of Administrator	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**	
Office of Air and Radiation	High	1	1	0	0	1	1	1	100%	0	0%	0	
	Moderate	11	1	1	0	12	1	0	0%	1	100%	0	
	Low	6	0	1	0	7	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**18**	**2**	**2**	**0**	**20**	**2**	**1**	50%	**1**	50%	**0**	
Office of Admininstration and Resource Management	High	0	0	0	0	0	0	0		0		0	
	Moderate	11	2	2	0	13	2	1	50%	1	50%	0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized		0	0	0	0	0	0		0		0	
	Sub-total	**11**	**2**	**2**	**0**	**13**	**2**	**1**	50%	**1**	50%	**0**	
Office of Chief Financial Officer	High	0	0	0	0	0	0	0		0		0	
	Moderate	16	4	0	0	16	4	3	75%	1	25%	0	
	Low	2	0	0	0	2	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**18**	**4**	**0**	**0**	**18**	**4**	**3**	75%	**1**	25%	**0**	
Office of Environmental Information	High	0	0	0	0	0	0	0		0		0	
	Moderate	16	0	6	1	22	1	1	100%	0	0%	0	
	Low	16	0	3	0	19	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**32**	**0**	**9**	**1**	**41**	**1**	**1**	100%	**0**		**0**	
Office of General Counsel	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**	
Office of International Activities	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**	
Office of Inspector General	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	1	0	0	7	1	1	100%	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	**8**	**1**	**0**	**0**	**8**	**1**	**1**	100%	**0**		**0**	
Office of Prevention Pesticides and Toxic Substances	High	0	0	0	0	0	0	0		0		0	
	Moderate	6	1	1	0	7	1	0	0%	1	100%	0	
	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**	**0**		**1**	100%	**0**	
Office of Research and Development	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	2	0	0	7	2	1	50%	1	50%	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**	**2**	**0**	**0**	**15**	**2**	**1**	50%	**1**	50%	**0**	
Office of Solid Waste and Emergency Response	High	0	0	0	0	0	0	0		0		0	
	Moderate	4	1	1	0	5	1	0		1	100%	0	
	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**	**0**		**1**	100%	**0**	
Office of Enforcement and Compliance Assurance	High	0	0	0	0	0	0	0		0		0	
	Moderate	8	1	0	0	8	1	0		1	100%	0	
	Low	3	0	0	0	3	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**11**	**1**	**0**	**0**	**11**	**1**	**0**		**1**	100%	**0**	
Office of Water	High	0	0	0	0	0	0	0		0		0	
	Moderate	8	1	0	0	8	1	0		1	100%	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**	**1**	**0**	**0**	**8**	**1**	**0**		**1**	100%	**0**	

Section C - Inspector General: Questions 1 and 2

Agency Name: Environmental Protection Agency **Submission date:** 21-Sep-07

		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	
Bureau Name	**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
Region 1	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**	
Region 2	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**	
Region 3	High	0	0	0	0	0	0	0		0		0	
	Moderate	1	1	0	0	1	1	1	100%	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**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**0**		**0**	
Region 4	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**	
Region 5	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**	
Region 6	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**	
Region 7	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**	
Region 8	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**	
Region 9	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**	
Region 10	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**	
Agency Totals	**High**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**0**	0%	**0**	
	Moderate	**109**	**15**	**12**	**1**	**121**	**16**	**8**	50%	**8**	50%	**0**	
	Low	**44**	**0**	**5**	**0**	**49**	**0**	**0**		**0**		**0**	
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**154**	**16**	**17**	**1**	**171**	**17**	**9**	53%	**8**	47%	**0**	

For each system selected for review, the OIG evaluated the system for compliance with either the Federal C&A or the security control testing requirements. As such, the percentage columns for questions 2a & b represent the percentage of systems evaluated in relationship to the total number of systems operated by the respective EPA program or regional office. Likewise, the percentage rate does not represent the rate in which the reviewed system complied with the evaluated Federal security requirement. The OIG did not test EPA systems for compliance with Federal contingency plan requirements.

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	Almost Always (96-100% 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)	Agency or Contractor system?

Number of known systems missing from inventory:	

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:

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	Satisfactory

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:	

Comment: The OIG evaluated nine EPA systems for compliance with selected Federal C&A requirements. Our review disclosed that all evaluated systems were complaint with the selected requirements. See question 5b for the evaluated C&A factors. Based on our limited review, we rated the Agency's C&A process as Satisfactory.

Section C - Inspector General: Questions 6 and 7

Agency Name: Environmental Protection Agency

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
	Comments: **The EPA has implemented a Privacy Impact Assessment (PIA) process. The procedures are available on the Agency's Intranet. The OIG's evaluation was based on whether applicable PIA guidance exist, was current, and available to the EPA personnel. The OIG did not test EPA's implementation of the PIA guidance.**	
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
	Comments: **The Agency has developed an interim policy to address safeguarding personnally identifiable information. Additionally, employees were made aware of the importance of safeguardning PII through the Agency's on-line FY2007 Information Security Awareness Training. However, the OIG has identified some areas where EPA could improve its practices for approving the download and access to PII. The OIG plans to issue a separate memorandum to the Chief Information Officer in October 2007 documenting our findings.**	

Question 7: Configuration Management

7.a.	**Is there an agency-wide security configuration policy? Yes or No.** **Comments**:	Yes
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **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	
	Comments: The OIG did not test EPA systems for compliance with NIST common security configurations. The OIG hired a contractor to evaluate EPA's standard configuration documents (SCD) against NIST requirements, if available, or industry best practices. The contractor noted that for all EPA SCDs selected for review, the SCD's content was consistent with a published authoritative document for securing the applicable operating system platform. However, the contractor identified that EPA should take steps to update six of the reviewed SCDs. Based on interviews with EPA officials, the contractor learnt that EPA is currently updating five of the SCDs in question. The contractor will provide EPA with the final analysis for each reviewed SCD in a separate document.	

Section C - Inspector General: Questions 8, 9, 10 and 11

Agency Name: Environmental Protection Agency

Question 8: 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.

8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes
	Comments:	

Question 9: 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 10: Peer-to-Peer File Sharing

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**

Question 11: E-Authentication Risk Assessments

The agency has completed system e-authentication risk assessments. Yes or No.	**No**

Comments: EPA has not completed e-authentication risk assesments for four applications.

Appendix A

Summary of Significant Fiscal Year 2007 Security Control Audits

During Fiscal Year 2007, the U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) initiated numerous audits of EPA's information technology security program and information systems. The following synopsizes key findings.

1. EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents, Report No. 2007-P-00007, January 11, 2007

EPA had not established procedures to ensure identification of all contractor systems. EPA has not ensured that information security requirements were accessible by the contractors and appropriately maintained. As a result, EPA system inventories may not include all appropriate contractor systems, and its contractors may not be implementing adequate security safeguards.

Although EPA offices were aware of the Agency's computer security incident response policy, many offices lacked local reporting procedures, had not fully implemented automated monitoring tools, and did not provide sufficient training on local procedures. EPA offices also did not have access to network attack trend information necessary to implement proactive defensive measures.

In response to our final report, Office of Environmental Information officials indicated that they had complete actions on four of the report recommendations. The Office of Environmental Information is continuing to work on updating the Agency's Information Security Manual, which will provide Agency officials procedures for determining when contractor information systems are subject to Federal information security requirements. EPA has also updated its Computer Security Incident Response Capability procedures to better define the local incident handling procedures. EPA indicated that it is also providing regular training to the information security community on prioritizing security incidents and escalating notifications

2. EPA Could Improve Controls Over Mainframe System Software, Report No. 2007-P-00008, January 29, 2007

The contractor that performed this review for the OIG identified several weaknesses in EPA's internal controls over its mainframe system software, including:

- Roles and responsibilities were not clearly assigned.
- Change controls were not performed in accordance with Agency policies.
- Policies, procedures, and guides could be strengthened.
- Security settings for sensitive datasets and programs were not effectively configured or implemented.

As a result of these weaknesses, EPA is exposed to greater risk since its mainframe system software could potentially be comprised.

3. EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance, Report No. 2007-P-00017, March 29, 2007

We discovered weaknesses in how EPA offices (1) monitor databases for known security vulnerabilities, (2) communicate the status of critical system patches, and (3) monitor the use of and access to database administrator accounts and privileges. These weaknesses exist because EPA had not implemented security processes to (1) actively monitor systems that share data with the Integrated Financial Management System, (2) share and collect information on the implementation of critical system patches, and (3) effectively manage access controls. Without these processes, the integrity of critical data in key Office of the Chief Financial Officer systems could be undermined. As a result, the Office of the Chief Financial Officer cannot ensure that the integrity of the data it provides to senior Agency officials is adequately protected. We also identified specific technical weaknesses in three of the financial databases that share data with the Integrated Financial Management System.

4. EPA Needs to Strengthen Its Privacy Program Management Controls, Report No. 2007-P-00035, September 17, 2007

EPA needs to set up a more comprehensive management control structure to govern and oversee the program. In particular, EPA needs to establish goals and activities for the Privacy Program and measure progress. Further, EPA needs to update its Privacy Program policies and establish processes to manage and make these policies available to responsible EPA personnel. Also, EPA needs to set up compliance and accountability processes to ensure adherence with key Privacy Program tenets. These weaknesses existed because of the low priority EPA managers placed on the Privacy Program. A major loss of privacy information could result in substantial harm, embarrassment, and inconvenience to individuals. It could lead to identity theft or other fraudulent use of the information, which in addition to harming the individuals involved could be costly to the Agency and its reputation.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Agency Followup Official
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Director, Office of Technology Operations and Planning
Senior Agency Information Security Officer
Acting Inspector General