OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Fiscal Year 2006 Federal Information Security Management Act Report

Status of EPA's Computer Security Program

Report No. 2006-S-00008

September 25, 2006

Report Contributors: Rudolph M. Brevard
Neven Morcos
William Coker
Warren Brooks
Sabrena Stewart

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

OFFICE OF
INSPECTOR GENERAL

September 25, 2006

MEMORANDUM

SUBJECT: Fiscal Year 2006 Federal Information Security Management Act Report

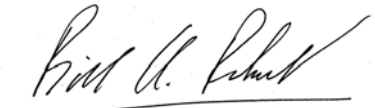
TO: Stephen L. Johnson
Administrator

Attached is the Office of Inspector General's (OIG's) Fiscal Year 2006 Federal Information Security Management Act Report, as prescribed by the Office of Management and Budget (OMB). This report includes the results of our annual security review and highlights the efforts to secure and protect the Agency's information assets.

Although the Agency has made substantial progress to improve its security program, the OIG identified weaknesses in the Agency's incident reporting practices. These weaknesses contribute to (1) the incident reporting program not being fully implemented and (2) all security incidents not being reported. As a result, the OIG answered "NO" to question 7a in the OMB reporting template. Also included is Appendix A, which synopsizes the results of our significant Fiscal Year 2006 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.

Sincerely,



Bill A. Roderick
Acting Inspector General

Attachment

cc: Assistant Administrator for Environmental Information and Chief Information Officer
Director, Office of Technology Operations and Planning
Senior Agency Information Security Officer

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

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 06 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 06 Agency Systems		b. FY 06 Contractor Systems		c. FY 06 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	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%**
Office of Air and Radiation	High	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	12	0	0	0	12	0	0	0.0%	0	0.0%	0	0.0%
	Low	6	0	2	0	8	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	**19**	**0**	**2**	**0**	**21**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Administration and Resource Management	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	10	0	2	0	12	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	**11**	**0**	**2**	**0**	**13**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Chief Financial Officer	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	16	2	0	0	16	2	2	100.0%	2	100.0%	2	100.0%
	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	**18**	**2**	**0**	**0**	**18**	**2**	**2**	**100.0%**	**2**	**100.0%**	**2**	**100.0%**
Office of Enforcement and Compliance Assurance	High	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	0	0	0	8	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	**11**	**0**	**0**	**0**	**11**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Environmental Information	High	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	17	0	5	0	22	0	0	0.0%	0	0.0%	0	0.0%
	Low	15	1	3	0	18	1	1	100.0%	1	100.0%	1	100.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**33**	**1**	**8**	**0**	**41**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**

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	0.0%
	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 Activiities	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	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	5	0	0	0	5	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	0.0%
	Moderate	7	0	0	0	7	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	**8**	**0**	**0**	**0**	**8**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Research and Development	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	0	0	0	8	0	0	0.0%	0	0.0%	0	0.0%
	Low	6	0	0	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	**14**	**0**	**0**	**0**	**14**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Solid Waste and Emergency Response	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	5	0	1	0	6	0	0	0.0%	0	0.0%	0	0.0%
	Low	4	0	2	1	6	1	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**	**0**	**3**	**1**	**12**	**1**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Office of Water	High	1	0	0	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	0	1	1	9	1	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	1	1	1	1	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**	**0**	**2**	**2**	**11**	**2**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 1	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 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%**
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	0.0%
	Moderate	1	0	0	0	1	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	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Region 9	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Moderate	1	0	1	1	2	1	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**	**1**	**1**	**2**	**1**	**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	**159**	**3**	**18**	**4**	**177**	**7**	**3**	**42.9%**	**3**	**42.9%**	**3**	**42.9%**
Agency Totals	**High**	**4**	**0**	**0**	**0**	**4**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**111**	**2**	**10**	**2**	**121**	**4**	**2**	**66.7%**	**2**	**66.7%**	**2**	**66.7%**
	Low	**44**	**1**	**8**	**2**	**52**	**3**	**1**	**33.3%**	**1**	**33.3%**	**1**	**33.3%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Total	**159**	**3**	**18**	**4**	**177**	**7**	**3**	**42.9%**	**3**	**42.9%**	**3**	**42.9%**

Comments: The Office of Inspector General (OIG) and the Agency agree on the number of EPA systems. The Agency is reporting 173 FISMA reportable systems and the OIG is reporting 177. The OIG identified four contractor systems that were not included in the Agency's inventory. Subsequent to the finding, the Agency included the four systems in its system inventory and categorized the sensitivity of the data in these systems. The Agency did not include the four systems in its final FISMA reporting numbers because the systems are currently being evaluated.

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 **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **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
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.a. Based on OIG work done to supplement FY 2006 FISMA, we found that the Agency needs to improve process for identifying and monitoring contractor systems. :		

Question 4

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

Comment: 4.e.

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 - -	- Satisfactory
Comments: EPA has sufficiently published C&A policies. However, we found the Agency's overall processes for implementing C&A policies and procedures need improvement. Proior audit work identified major applications without up-to-date authorizations to operate, risk assessments, and other key security documents.	

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

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	
Windows 2000 Professional	Yes	Yes	
Windows 2000 Server	Yes	Yes	
Windows 2003 Server	Yes	Yes	
Solaris	Yes	Yes	
HP-UX	N/A	No	
Linux	Yes	Yes	
Cisco Router IOS	Yes	Yes	
Oracle	Yes	Yes	
Other. Specify:			

Comments: We did not conduct audit work to determine the extent of the Agency's implementation of the above operating systems. The OIG has programmed an operating system review in its FY07 audit plan.

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.	No
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: EPA has established Agency-wide policies and procedures for reporting security incidents. However, we found in supplementing our FY 2006 FISMA audit that EPA needs to take further steps to (1) implement its incident handling program to ensure all violations are consistently reported; (2) develop and train personnel on local incident reporting procedures; (3) implement its centralized virus/spyware/malware reporting system, and (4) make security trend information available. We plan to issue a separate report on EPA's incident reporting practices in November 2006.		
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	- Almost Always, or approximately 96-100% of employees have sufficient training
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
Comments:		

Appendix A

Summary of Significant Fiscal 2006 Security Control Audits

During Fiscal Year 2006, EPA's Office of Inspector General (OIG) initiated numerous audits of EPA's information technology security program and information systems. The following summary synopsizes key objectives and findings. Copies of all final reports are located on the OIG's Internet site at *http://www.epa.gov/oig/publications.htm*.

1. EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes, Report No. 2006-P-00002, October 17, 2005

We found that program offices had not effectively implemented processes to comply with Federal and EPA requirements related to information security. We found major applications without (1) adequate certification and accreditation, (2) contingency plans or testing of the plans, and (3) a process to monitor for known security vulnerabilities. As such, all security control deficiencies are not reported in EPA's Plans of Action and Milestones system. EPA could have discovered these security deficiencies had it implemented processes to verify and validate offices' compliance with established Federal and Agency requirements. Therefore, the Chief Information Officer is not receiving timely and accurate information with which to plan, implement, evaluate, and report EPA's information technology security status and security remediation activities to the Office of Management and Budget.

2. EPA Could Improve Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus, Report No. 2006-P-00005, December 14, 2005

The OIG contracted with KPMG, LLP, to audit physical access controls and service continuity/contingency planning controls for select financial and mixed-financial systems hosted at EPA's Research Triangle Park campus. KPMG found that controls needed to be improved in areas such as visitor access to facilities, use of contractor access badges, and general physical access to the National Computer Center, computer rooms outside the Center, and media storage rooms.

Controls also needed improvement in areas such as completing a business impact analysis, application contingency plans, authorizing to move backup data between key facilities, and environmental controls. In many cases, EPA has in place compensating controls that help reduce the risk of the above issues. However, KPMG believes that controls can be improved to further reduce the risks.

3. Information Security Series: Security Practices

We evaluated the information security practices of five Agency program offices. For each selected application, we evaluated the following security controls: certification and accreditation practices, application contingency plans, and processes used to test and evaluate security controls. Although the EPA offices complied with many of the reviewed security requirements, they needed to improve information security practices to ensure that (1) key security documents are kept current whenever the system undergoes a major modification or significant change in processing and (2) risk assessments and contingency plans are developed and tested in a timely manner. EPA offices could improve processes to ensure production servers are actively monitored for known security vulnerabilities.

We issued the following five reports under this series:

- *Integrated Contract Management System*, Report No. 2006-P-00010, January 31, 2006
- *Comprehensive Environmental Response, Compensation, and Liability Information System*, Report No. 2006-P-00019, March 28, 2006
- *Integrated Compliance Information System*, Report No. 2006-P-00020, March 29, 2006
- *Safe Drinking Water Information System*, Report No. 2006-P-00021, March 30, 2006
- *Clean Air Markets Division Business System*, Report No. 2006-P-00024, May 4, 2006

4. Controls over Mainframe System Software

The overall objective was to determine the effectiveness of information system controls over the configuration of, access to, and modification of mainframe system software (including all operating systems, utilities, and security software) residing at the EPA's National Computer Center. We plan to issue the final report in October 2006.

5. Management Controls over Contractor-owned Systems that Contain EPA Data and Incident Reporting

We sought to determine whether EPA defined security requirements for contractor owned systems that collect information on EPA's behalf. We also sought to determine whether EPA offices identified and reported all security incidents to EPA's Computer Security Incident Response Capability, which is EPA's computer security incident reporting process. We plan to issue the final report in November 2006.

Appendix B

Distribution

Office of the Administrator
Acting 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
Acting Inspector General