U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Briefing Report: Improvements Needed in EPA's Information Security Program

Report No. 13-P-0257 **May 13, 2013**

Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Cheryl Reid
Vincent Campbell
Neven Soliman
Albert E. Schmidt
Rodney Allison
Nii-Lantei Lamptey
Kyle Denning

Abbreviations

CERT	Computer Emergency Response Team
EPA	U.S. Environmental Protection Agency
FDCC	Federal Desktop Core Configurations
FISMA	Federal Information Security Management Act
OCSPP	Office of Chemical Safety and Pollution Prevention
OEI	Office of Environmental Information
POA&M	Plan of Action and Milestones
TSCA	Toxic Substances Control Act
USGCB	U.S. Government Configuration Baseline

U.S. Environmental Protection Agency
Office of Inspector General

13-P-0257
May 13, 2013

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) prepared this supplemental report to document the details, and make recommendations, for weaknesses the OIG identified during its review of the Agency's information security program and practices. That review was conducted as required by the Federal Information Security Management Act (FISMA), which requires inspectors general to prepare an annual evaluation of their agencies' information security programs and practices. The Department of Homeland Security issued reporting guidelines documenting 11 FISMA reporting metrics to be evaluated as part of the fiscal year 2012 FISMA audit.

This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthen EPA's Workforce and Capabilities.*

For further information, contact our Office of Congressional and Public Affairs at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2013/20130513-13-P-0257.pdf

Briefing Report: Improvements Needed in EPA's Information Security Program

What We Found

We found weaknesses in the following Agency programs regarding its information security program and practices:

- Continuous monitoring management
- Configuration management
- Risk management
- Plan of action and milestones
- Contractor systems

This supplemental report to our previously issued report, *Fiscal Year 2012 Federal Information Security Management Act Report: Status of EPA's Computer Security Program* (Report No. 13-P-0032), issued October 26, 2012, provides additional detailed information for the above weaknesses.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Environmental Information implement the continuous monitoring activities as specified in the Agency's Continuous Monitoring Strategic Plan, document the remediation of configuration-related vulnerabilities, and implement a strategic plan for EPA's risk management framework.

The Agency concurred with the report's recommendations and provided high-level planned corrective actions with completion dates. The Agency needs to provide a completion date for one planned corrective action and additional information on how the EPA will verify that offices remediate identified weaknesses.

Noteworthy Achievements

The Office of Environmental Information has developed a strategic plan for continuous monitoring, approved the risk management framework, and created a Risk Executive Group tasked with developing an Agency-wide risk management strategy.

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

THE INSPECTOR GENERAL

May 13, 2013

MEMORANDUM

SUBJECT: Briefing Report: Improvements Needed in EPA's Information Security Program
Report No. 13-P-0257

FROM: Arthur A. Elkins Jr.

TO: Malcolm D. Jackson, Assistant Administrator and Chief Information Officer
Office of Environmental Information

This is our report on the subject evaluation conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the EPA position. The Agency concurred with the report's recommendations and provided high-level planned corrective actions with completion dates. However, the Agency needs to provide a completion date for one planned corrective action and revise another planned corrective action to fully address the report's recommendation. Therefore, the responses to those two recommendations are considered unresolved. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 60 calendar days. You should include planned corrective actions and completion dates for all unresolved recommendations. Your response will be posted on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification. We have no objections to the further release of this report to the public. We will post this report to our website at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact Richard Eyermann, Acting Assistant Inspector General for Audit, at (202) 566-0565 or eyermann.rich@epa.gov; or Rudolph M. Brevard, Director, Information Resources Management Audits, at (202) 566-0893 or brevard.rudy@epa.gov.

Improvements Needed in EPA's Information Security Program

Results of Review

Purpose

The Federal Information Security Management Act (FISMA) requires inspectors general to perform an annual evaluation of their agencies' information security programs and practices. We found information security weaknesses during our fiscal year 2012 FISMA audit of the U.S. Environmental Protection Agency (EPA). This briefing report provides the details for the weaknesses found during the FISMA audit.

Scope and Methodology

This is a supplemental draft report based on the fiscal year 2012 FISMA audit. We conducted the FISMA audit work at EPA headquarters in Washington, D.C.; the National Computer Center, Research Triangle Park, North Carolina; and all 10 regions. This audit was conducted from February 2012 through November 2012. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Scope and Methodology (Cont.)

We reviewed federal regulations and EPA policies and procedures. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of EPA's operations. We also conducted limited tests of selected information system security controls.

Scope and Methodology (Cont.)

For fiscal year 2012, we conducted an overall assessment for the following 11 FISMA metrics:

1. Continuous monitoring management
2. Configuration management
3. Identity and access management
4. Incident response and reporting
5. Risk management
6. Security training
7. Plan of action and milestones
8. Remote access management
9. Contingency planning
10. Contractor systems
11. Security capital planning

Continuous Monitoring Management

In June 2012 EPA developed the Continuous Monitoring Strategic Plan. However, the Agency continues working toward implementing the plan's continuous monitoring that includes ongoing assessments of security controls.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

1. Implement the continuous monitoring activities as specified in the Agency's Continuous Monitoring Strategic Plan.

Continuous Monitoring Management (Cont.)

Agency Response and OIG Evaluation

The Agency concurs with the recommendation and provided a planned corrective action, but the Agency did not provide a planned completion date. The OIG considers the Agency's response unresolved until a completion date has been established.

Configuration Management

- EPA is not assessing baseline compliance for EPA's firewalls, routers, and Web server software.
- EPA did not have a process for timely remediation of configuration compliance scans.
- EPA did not fully implement Federal Desktop Core Configurations/U.S. Government Configuration Baseline (FDCC/USGCB) secure configuration settings for 4 out of 15 workstations selected for testing.
- EPA does not have a specified, documented timeline to correct deviations from baseline configurations.

Configuration Management (Cont.)

- EPA did not ensure that unauthorized firewall rule modifications occurred.

- EPA has configuration management policies and procedures. However, the procedures did not provide guidance as to what the program offices and regions should classify as configuration items (i.e., hardware, software, firmware) for information systems, and did not provide a timeline of the system's development life cycle.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

2. Assess baseline compliance for EPA's firewalls, routers, and Web servers software.

3. Update the configuration management process to verify program offices remediate FDCC/USGCB deviations in a timely manner.

4. Perform regular reviews of firewall rules to ensure no unauthorized changes were made.

Recommendations (Cont.)

5. Update configuration management procedures to define what the program offices and regions should classify as configuration items for information systems, and define when during the system development life cycle the configurable items are to be placed under configuration management.

Agency Response and OIG Evaluation

The Agency concurs with the recommendations and provided planned corrective actions and completion dates, but the planned action does not fully address recommendation 3. The planned action does not include a verification procedure to confirm that program offices actually remediate FDCC/USGCB deviations in a timely manner.

Risk Management

- Senior EPA officials throughout the Agency are currently not briefed on:
  - Mission/business-specific risks and organizational level (strategic) risks.
  - Threat activity described in U.S. Computer Emergency Response Team's (CERT's) cyber-security threat reports.
- Although the risk management framework has been approved, the strategic plan needs to be implemented (e.g., the strategic plan cites "security controls need to be implemented and verified").

Risk Management (Cont.)

- EPA has recently approved the establishment of a Risk Executive Group. However, the group needs to:
  - Define the core mission and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations).
  - Define both the types of information that the organization needs in order to successfully execute the stated missions and business processes and the internal and external information flows.
  - Specify the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Risk Management (Cont.)

- Specify the types and extent of risk mitigation measures the organization plans to employ to address identified risks.
- Specify how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation.
- Specify the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

6. Brief senior EPA officials throughout the Agency on information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks, and threat activity described in U.S. CERT cyber-security threat reports.

7. Implement a strategic plan for EPA's risk management framework.

Recommendations (Cont.)

8. Work with the Risk Executive Group to:

   a. Define the core mission and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations).
   b. Identify the types of information that the organization needs in order to successfully execute the stated missions and business processes.
   c. Specify the degree of autonomy for subordinate organizations that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Recommendations (Cont.)

d. Specify the types and extent of risk mitigation measures the organization plans to employ to address identified risks.
e. Specify how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation.

Agency Response and OIG Evaluation

The Agency concurs with the recommendations and provided planned corrective action with completion dates for each recommendation. The OIG concurs with the planned actions.

Plan of Action and Milestones

EPA does not have plan of action and milestones (POA&M) procedures or processes that provide assurance that the weaknesses identified have been corrected by the planned remediation.

Recommendation

We recommend that the Assistant Administrator for Environmental Information:

9. Implement POA&M procedures to verify that weaknesses identified in POA&Ms are corrected by the planned remediation.

Plan of Action and Milestones (Cont.)

Agency Response and OIG Evaluation

The Agency concurs with the recommendation and provided a planned corrective action with a completion date. The OIG concurs with the planned action.

Contractor Systems

The Office of Chemical Safety and Pollution Prevention (OCSPP) did not complete the required annual assessment of security controls for the Toxic Substances Control Act (TSCA) Online system. As of August 2012, OCSPP had assessed only 1.35% of the security controls.

OCSPP personnel stated that in August 2010 they submitted a request to the Office of Environmental Information (OEI) to have the system removed from Office of Management and Budget reporting. OCSPP personnel stated that even though the OEI did not provide a formal response, they were under the impression that their request was granted when advised to add tasks in the EPA's Automated System Security Evaluation and Remediation Tracking system to close out the system.

Contractor Systems (Cont.)

OCSPP personnel stated that they have not completed an assessment of security controls on the system since August 2010. OCSPP personnel stated that in March 2012 OEI informed them that the system could not be removed. OCSPP informed the OIG that contractor services have been obtained to perform a risk assessment and certification and accreditation for the system.

Recommendation

We recommend that the Assistant Administrator for Environmental Information:

10. Verify that OCSPP completed an assessment of security controls for the TSCA Online system.

Contractor Systems (Cont.)

Agency Response and OIG Evaluation

The Agency concurs with the recommendation and provided a planned corrective action with a completion date. The OIG concurs with the planned action.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
1	6	Implement the continuous monitoring activities as specified in the Agency's Continuous Monitoring Strategic Plan.	U	Assistant Administrator for Environmental Information			
2	10	Assess baseline compliance for EPA's firewalls, routers, and Web servers software.	O	Assistant Administrator for Environmental Information	09/30/2013		
3	10	Update the configuration management process to verify program offices remediate FDCC/USGCB deviations in a timely manner.	U	Assistant Administrator for Environmental Information			
4	10	Perform regular reviews of firewall rules to ensure no unauthorized changes were made.	O	Assistant Administrator for Environmental Information	09/30/2013		
5	11	Update configuration management procedures to define what the program offices and regions should classify as configuration items for information systems, and define when during the system development life cycle the configurable items are to be placed under configuration management.	O	Assistant Administrator for Environmental Information	06/28/2013		
6	15	Brief senior EPA officials throughout the Agency on information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks, and threat activity described in U.S. CERT cyber-security threat reports.	O	Assistant Administrator for Environmental Information	06/30/2103		
7	15	Implement a strategic plan for EPA's risk management framework.	O	Assistant Administrator for Environmental Information	12/31/2013		
8	16	Work with the Risk Executive Group to:	O	Assistant Administrator for Environmental Information	12/31/2013		
	16	a. Define the core mission and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations).					
	16	b. Identify the types of information that the organization needs in order to successfully execute the stated missions and business processes.					
	16	c. Specify the degree of autonomy for subordinate organizations that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.					
	17	d. Specify the types and extent of risk mitigation measures the organization plans to employ to address identified risks.					

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
	17	e. Specify how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation.					
9	18	Implement POA&M procedures to verify that weaknesses identified in POA&Ms are corrected by the planned remediation.	O	Assistant Administrator for Environmental Information	06/30/2013		
10	21	Verify that OCSPP personnel complete an assessment of security controls for the TSCA Online system.	O	Assistant Administrator for Environmental Information	09/06/2013		

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is unresolved with resolution efforts in progress

Agency Response to Draft Report

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

OFFICE OF
ENVIRONMENTAL INFORMATION

4/19/2013

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OMS-FY12-0003 "Briefing Report: Improvements Needed in EPA's Information Security Program," dated March 6, 2013

FROM: Malcolm D. Jackson
Assistant Administrator and Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the agency's overall position, along with its position on each of the report recommendations. For those report recommendations with which the agency agrees, we have provided high-level intended corrective actions and estimated completion dates.

AGENCY'S OVERALL POSITION

Senior Agency Information Security Officer Response

The report facts are accurate with regard to the areas the Senior Agency Information Security Officer (SAISO) has direct insight or access to the underlying information with the following exceptions. Under the Risk Management section, the Office of Inspector General (OIG) did not define what roles are considered 'Senior EPA officials' nor which U.S. Computer Emergency Response Team's (CERT) cyber security threat reports are in scope for these officials. The assumption is that the OIG is not stating that all U.S. CERT threat reports should be briefed to senior officials since the majority of the reports are technical in nature and too low level to be useful for 'senior officials.' Also, the assumption is that the OIG did not intend to include system administrators, Information Security Officers and other such roles as senior officials to whom these technical, low level reports would be appropriate.

EPA defines 'Senior Officials' as the Deputy Administrator, Chief Information Officer (CIO), and Deputy CIO. These roles receive threat briefs at a level appropriate for senior officials that enable them to manage strategic risks. EPA Authorizing Officials – those roles accepting risk at the system and mission level – receive appropriate mission and system level risk briefs through the system authorization process. Information Security Officers (ISOs) periodically receive U.S. CERT threat briefs as well as threat briefs from the EPA CSIRC. The ISOs and others in EPA also have available to them daily threat reports provided by a U.S. CERT source provider. Given the defined scopes of senior officials and threat briefs above, the SAISO believes the agency is complying with recommendations 6 through 10.

Office of Environmental Information, Office of Technology Operations and Planning Response
The Office of Technology Operations and Planning (OTOP) agrees with the Office of Inspector General's (OIG) recommendations affecting resources under OTOP's purview and have provided high-level intended corrective actions and estimated completion dates for recommendations 1 through 5.

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
1	Implement the continuous monitoring activities as specified in the Agency's Continues Strategic Plan.	OTOP is responsible for implementing the Continuous Monitoring (CM) activities in the Agency's CM Strategic Plan. A high level gap analysis has been performed and OTOP management is reviewing the findings for further action to include task designation among the	TBD

2	Assess baseline compliance for EPA's firewalls, routers, and web server's software.	OTOP/NCC will: Procure 3rd party independent assessment to formally review baseline. Add NIST 800-53 control, CM-02 as point of emphasis during future risk assessments.	FY13 QTR 4 (September 30, 2013)
3	Update the configuration management process to verify program offices remediate FDCC/USGCB deviations in a timely manner.	OTOP/EDSD, with input from the SAISO, will provide training and procedures for the Tivoli Endpoint Administrators to run compliance reports that will show FDCC/USGCB deviations for their respective program or regional office.	FY13 QTR 4 (September 6, 2013)
4	Perform regular reviews of firewall rules to ensure no unauthorized changes were made.	OTOP/NCC will review and recommend a practical solution for firewall rule reviews and integrity correlations. The implementation schedule will be assessed and determined based on approved solution and resource constraints.	FY13 QTR 4 (September 30, 2013)
5	Update configuration management procedures to define what the program offices and regions should classify as configuration items for information systems, and define when during the system development life cycle the configurable items are to be placed under configuration management.	OTOP will: Identify standard guidance for identifying IT configuration items based on best practices. OTOP will update the Configuration Management procedure.	FY13 QTR 3 (April 15, 2013) FY13 QTR 3 (June 28, 2013)

6	Brief senior EPA officials throughout the Agency on information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks, and threat activity described in U.S. CERT cyber-security threat reports.	The SAISO concurs with the following recommendations and plans to take stated actions	FY13 QTR 3 (June 30, 2013)
7	Implement a strategic plan for EPA's risk management framework.	The CIO's office will finalize and begin implementing a Risk Managment Strategic Plan by the end of Q1FY14	FY14 QTR 1 (December 31, 2013)
8	Work with the Risk Executive Group to: a. Define the core mission and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations). b. Identify the types of information that the organization needs in order to successfully execute the stated missions and business processes. c. Specify the degree of autonomy for subordinate organizations that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk. d. Specify the types and extent of risk mitigation measures the organization plans to employ to address identified risks. e. Specify how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation.	The CIO's office will finalize and begin implementing a Risk Managment Strategic Plan by the end of Q1FY14. This work will be accomplished in the development and implementation of the Risk Management Strategic Plan.	FY14 QTR 1 (December 31, 2013)

9	Implement POA&M procedures to verify that weaknesses identified in POA&Ms are corrected by the planned remediation.	The SAISO will implement a Plans of Actions and Milestones (POA&M) validation and monitoring process in Q3FY13.	FY13 QTR 3 (June 30, 2013)
10	Verify that OCSPP completed an assessment of security controls for the TSCA Online system.	The SAISO will verify OCSSP has completed security controls assessment on TSCA Online by the end of Q4FY13.	FY13 QTR 4 (September 6, 2013)

If you have any questions or concerns about this response, please feel free to contact Tom Tracy, Acting Director of the Policy, Outreach and Communications Staff, at (202) 564-6518 or Scott Dockum the OEI Audit Follow-up Coordinator at (202) 566-1914.

cc:

Robert McKinney
Anne Mangiafico
Brenda Young
Thomas Tracy
Scott Dockum

Appendix B

Distribution

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