


MEMORANDUM

SUBJECT: Response to Office of Inspector General Final Report No. 13-P-0257, "Briefing Report: Improvements Needed in EPA's Information Security Program," dated May 13, 2013

FROM: Renee P. Wynn 
Acting Assistant Administrator and Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the Final Audit Report on improving EPA's Information Security Program. As an update to the response we provided on the Draft Report in April, OEI has edited the attached list of corrective actions to include the following updates as identified in the Final Report:

- Recommendation 1 – an estimated due date has been added;
- Recommendation 3 – revised text has been added on the plan to meet to update the configuration management process, along with an estimated completion date;
- Recommendation 6 – updated to show that the completion date has been met; and,
- Recommendation 9 – updated to show that the completion date has been met.

If you have any questions or concerns about this response, please feel free to contact Jeffrey Worthington, Acting Director of the Policy, Outreach and Communications Staff, at (202) 566-0995 or Scott Dockum the OEI Audit Follow-up Coordinator at (202) 566-1914.

cc: Robert McKinney
Anne Mangiafico
Brenda Young
Jeffrey Worthington
Scott Dockum

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

| 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/TISS will implement 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 various divisions for implementation. | FY14 QTR 1 (December 31, 2013) |
| 2 | Assess baseline compliance for EPA's firewalls, routers, and web server's software. | OTOP/NCC will: <ul style="list-style-type: none"> • 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. | <p>OTOP/TISS will generate periodic reports depicting compliance status of assets shown in BigFix. As this is an ongoing effort, the planned completion date references the date in which the first compliance report will be generated from BigFix and in which non compliance tickets will be inserted into REMEDY.</p> <p>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.</p> <p>The deviations from the standards will be reported via tools to the SAISO and risk management and compliancy processes will apply – that is, recommendations will be provided to the CIO and the Risk Executive Group by the SAISO, reports will be provided to the SIO's and CIO, and Plans of Actions and Milestones (POA&M) will be monitored and validated by the SAISO. OTOP may implement network isolation etc., as a result of</p> | FY13 QTR 4 (September 30, 2013) |

| No. | Recommendation | High-Level Intended Corrective Action(s) | Estimated Completion by Quarter and FY |
|-----|--|--|---|
| | | CIO/risk management decisions. | |
| 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: <ul style="list-style-type: none"> • Identify standard guidance for identifying IT configuration items based on best practices. • OTOP will update the Configuration Management procedure. | Completed FY13 QTR 3 (April 15, 2013) Completed FY13 QTR 3 (June 28, 2013); (see appendix B of the EPA Configuration Management Procedure) |
| 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. | Completed 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 Management Strategic Plan by the end of Q1FY14. | FY14 QTR 1 (December 31, 2013) |
| 8 | Work with the Risk Executive Group to: <ol style="list-style-type: none"> a. Define the core mission and business processes for the | The CIO's office will finalize and begin implementing a Risk Management Strategic Plan by the end of Q1FY14. This work will be accomplished in the development and implementation of the Risk | FY14 QTR 1 (December 31, 2013) |

| No. | Recommendation | High-Level Intended Corrective Action(s) | Estimated Completion by Quarter and FY |
|-----|---|---|--|
| | <p>organization (including any derivative or related missions and business processes carried out by subordinate organizations).</p> <p>b. Identify the types of information that the organization needs in order to successfully execute the stated missions and business processes.</p> <p>c. Specify the degree of autonomy for subordinate organizations that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.</p> <p>d. Specify the types and extent of risk mitigation measures the organization plans to employ to address identified risks.</p> <p>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.</p> | Management Strategic Plan. | |
| 9 | Implement POA&M procedures to verify that weaknesses identified in POA&Ms are corrected by the planned remediation. | The SAISO will implement a POA&M validation and monitoring process in Q3FY13. | Completed FY13 QTR 3 (June 30, 2013) |

| No. | Recommendation | High-Level Intended Corrective Action(s) | Estimated Completion by Quarter and FY |
|------------|---|---|---|
| 10 | Verify that OCSP 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) |