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

DEC 2 1 2012

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: OEI's Response to OIG's Final Report – Office of Environmental Information Improvements Needed in EPA's Network Security Monitoring Program (12-P-0899)

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

TO: Arthur A. Elkins, Jr.
Inspector General

In response to the Final Audit Report, "Improvements Needed in EPA's Network Security Monitoring Program (12-P-0899), the Office of Environmental Information is pleased to provide you with our response to the OIG recommendations found in the report.

If you have any questions, please contact Robbie Young, Acting Director of the Policy and Program Development Staff, at (202) 566-2174.

Attachment

cc: James McDonald
Robbie Young
Scott Dockum

Office of Environmental Information / OTOP
Corrective Action Plan

Auditing Group: OIG
Audit No.: 12-P-0899
Final Report Date: September 27, 2012
OEI Lead Offices: OTOP & SAISO

Audit Title: Improvements Needed in EPA's Network Security Monitoring Program

OEI Leads and Phone: OTOP - Anne Mangiafico 202-564-9483;
SAISO – Robert McKinney (202) 564-0921

Recommendation	Corrective Action	Planned Completion Date	Status	POC for Recommendation	Comments	Concur Yes/No
1: Develop and implement a strategy with milestone dates to incorporate EPA's headquarters program offices within the SIEM environment.	OTOP/TISS will refine the project plan to reflect a thorough strategy for incorporating Program Offices into the SIEM environment. This strategy will include milestone dates for all Program Offices not already in SIEM.	12/31/13	In Progress - Implementing Program Office devices into ArcSight is currently underway as part of the overall strategy. A project plan exists that lists each Program Office.	OTOP/TISS Lee Kelly	There are multiple Program Offices already in ArcSight. Along with the Regional offices, other Program Offices are in various stages (Initial contact; Information Gathering; Testing; etc.) regarding implementation. It should be noted that ArcSight implementation is by licensed devices and requires budgetary resources that have to be approved and appropriated before all Regions/Program Offices will be implemented.	Yes
2: Develop and implement a formal training program that will meet EPA's information security staff needs in using the	OTOP/TISS will further codify the training program for ArcSight by documenting evidence of training for users	12/31/12	In Progress – A user guide has been developed and made available to users. Efforts	OTOP/TISS Lee Kelly	Training on ArcSight is accomplished by various methods. (1) Upon being granted access to ArcSight a one-on-one session is scheduled with the user to	Yes

SIEM tool. The training program should include a user guide on using the SIEM tool to generate reports and developing customized reports for filtering known and suspicious events.	and formalizing training requirements for ArcSight access.		moving forward will focus on refining the user guide and formalizing the training program.		go over the interface, basic/advanced searches, reports (default and custom) and queries among other items. This session usually lasts between 60-90 minutes. (2) Hewlett Packard (ArcSight manufacturer) also provides training courses on ArcSight on a fee-based schedule available from their website. (3) At the monthly ArcSight user group meeting demonstrations are held on how to perform certain functions and the users have an opportunity to ask questions on that topic. A user guide that includes chapters on reports and searches has been posted to the EPA SIEM collaboration page. This information was announced at the last user group meeting.	
3: Develop a policy or revise the Agency's Information Security Policy to comply with NIST SP 800-92. This policy should include, but not be limited to, defining log storage and disposal requirements, roles, and	Interim procedures were promulgated that provides guidance consistent with NIST SP 800-92	8/6/2012	Completed	SAISO	NA	Yes

responsibilities for the log management infrastructure.						
4: Finalize the SIEM tool's "Enterprise Reference Guide."	OTOP/TISS will review the Enterprise Reference Guide to determine gaps between its guidance and the current status of the SIEM project. The Enterprise Reference Guide will be updated and finalized, and referenced in other TISS/CSIRC operating procedures if necessary.	3/29/13	In Progress	OTOP/TISS Lee Kelly	The baseline document should be completed by the completion date. This document is dynamic in nature and will to some degree depend on actions/approvals as listed in Item 1 above.	Yes
5: Issue a memorandum to OEI officials requiring the SAISO be the addressee on all internal security reports and reviews in order to ensure identified weaknesses are recorded within the Agency's security weakness tracking system.	The SAISO promulgated a memo requiring all internal security reports and reviews be provided to the SAISO in order to ensure identified weaknesses are recorded within the Agency's security weakness tracking system.	11/1/2012	Completed	SAISO	NA	Yes
6: Create POA&Ms for all recommendations applicable to Agency internal reports identified in Appendix B.	POA&Ms were entered into the POA&M tracking tool for all SAISO applicable outstanding recommendations to Agency internal	12/18/2012	Completed	SAISO	NA	Yes

	reports identified in Appendix B.					
7: Develop and implement a process to verify that identified weaknesses in Appendix B are addressed and decisions are documented on actions taken.	The SAISO created and implemented a Monitoring and Validation Process for POA&Ms for EPA.	11/1/2012	Completed	SAISO	NA	Yes
8: Develop and implement a process to verify that regions and program office staff address vulnerabilities from NCC scans.	OTOP/NCC will ensure the SAISO's office and ISOs have access to all agency server vulnerability findings resulting from NCC scans. NCC's standard operating procedure will be updated to reflect ISO oversight responsibilities for ensuring vulnerabilities are remediated in 30 days or appropriate POA&Ms are put in place. The SAISO's office will verify POA&Ms are entered based on the vulnerability report findings then validate actions were taken to address the POA&Ms.	2/15/2013	In Progress	OTOP/NCC John Gibson	NA	Yes