



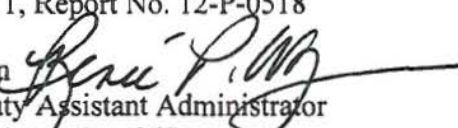
UNITED STATES ENVIRONMENTAL PROTECTION AGENCY  
WASHINGTON, D.C. 20460

JUL 11 2012

OFFICE OF  
ENVIRONMENTAL INFORMATION

**MEMORANDUM**

**SUBJECT:** OEI Response Report: Results of Technical Network Vulnerability Assessment:  
EPA's Region 1, Report No. 12-P-0518

**FROM:** Renee P. Wynn   
Principal Deputy Assistant Administrator  
and Senior Information Officer

**TO:** Arthur Elkins  
Inspector General

The purpose of this memorandum is to provide a response to the subject report and provide status regarding the Office of Environmental Information's (OEI) management of devices managed by our organization that reside on Region 1's network.

OEI appreciates the OIG's desire to ensure EPA has adequate controls for safeguarding devices from vulnerabilities and oversight.

Attached please find OEI's detailed response to OIG's current report. As outlined in the attached response, OEI agrees in part with the recommendations and have outlined a plan to address the vulnerabilities found during the assessment of Region 1.

If you have any questions, please feel free to contact me.

Attachment

cc: Rudy Brevard, Product Line Director, Information Resources Management Assessments  
Patricia Hill, Assistant Inspector General for Mission Systems  
Vaughn Noga, Director, Office of Technology Operations and Planning  
Maja Lee, Acting Director, Enterprise Desktop Solutions Division  
Scott Dockum, OEI Audit Follow-up Coordinator  
Anne Mangiafico, OTO Audit Coordinator

**Office of Environmental Information  
Corrective Action Plan  
As of 07/02/12**

<b>Auditing Group: OIG</b> <b>Audit No.: 12-P-0518</b> <b>Report Date: June 5, 2012</b> <b>OEI Lead Office: OTOP/EDSD</b>	<b>Audit Title: Draft Report – Results of Technical Network Vulnerability Assessment: EPA’s Region 1</b> <b>OEI Lead and Phone: Mark Hubbard 202-564-8376</b>
--	--

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
<b>1-1:</b> Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings.		See below for corrective actions recommendations a, b and c.		
<b>1-1a:</b> High vulnerability consists of the following: Bos-s1bb-wism1a.r01.wireless.epa.gov and Bos-s2bb-wism1a.r01.wireless.epa.gov, Vulnerability found 10264 - SNMP Agent Default Community Names		<b>Concur/Completed</b> The Simple Network Management Protocol (SNMP) default community strings were removed.		
<b>1-1b:</b> High vulnerability consists of the following: Bigfix 1 DRAC and Bigfix 2 DRAC, Vulnerability found 10264 - SNMP Agent Default Community Names		<b>Non-Concur in Part</b> EDSD non-concurs with the SNMP Agent Default Community Strings vulnerability and has deemed this as a false positive. The community strings are set in a manner that allows the BigFix	7/05/2012	

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
		<p>relay servers to communicate with each other and a screen shot will be provided that shows these attributes.</p> <p>The following POAM will be placed in the Agency's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) system to reflect EDSD's planned actions.</p> <ul style="list-style-type: none"> <li>• Vulnerability 57582 - SSL Self-Signed Certificate has been escalated to Dell and a solution is being engineered at this time. The EDSD ISO will update ASSERT to reflect implementation of a solution of this vulnerability.</li> </ul>		
<p><b>1-1c:</b> Medium vulnerability consists of the following:  10539 - DNS Server Recursive Query Cache Poisoning Weakness, 12217 - DNS Server Cache Snooping Remote Information Disclosure.</p>		<p><b>Non-Concur</b>  The vulnerability shown from the scan was done on a recursive nameserver and by functionality this is what the server is supposed to do. In general this finding isn't aimed at this type of the</p>		

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
		Domain Named System (DNS) server and is meant for external facing DNS servers.		
2-1: Create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities according to Agency procedures.		<b>Concur</b> The EDSO ISO will add additional POAMs in ASSERT to track these findings and solutions	7/05/2012	
3-1: Perform a technical vulnerability assessment test of assigned network resources within 60 days to confirm completion of remediation activities.		<b>Concur</b> The EDSO ISO will work with the Technology and Information and System Security (TISS) staff to conduct a Validation and Verification scan on the devices EDSO owns.	8/02/2012	