U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Results of Technical Network Vulnerability Assessment: EPA's National Vehicle and Fuel Emissions Laboratory

Report No. 12-P-0900 **September 27, 2012**

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

Report Contributors: Rudolph M. Brevard
Warren Brooks
Scott Sammons

Hotline

To report fraud, waste, or abuse, contact us through one of the following methods:

e-mail: OIG_Hotline@epa.gov
phone: 1-888-546-8740
fax: 202-566-2599
online: http://www.epa.gov/oig/hotline.htm

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue NW
Mailcode 2431T
Washington, DC 20460

U.S. Environmental Protection Agency
Office of Inspector General

12-P-0900
September 27, 2012

At a Glance

Why We Did This Review

We sought to conduct network vulnerability testing of the U.S. Environmental Protection Agency's (EPA's) National Vehicle and Fuel Emissions Laboratory (NVFEL) Local Area Network to identify resources that contained commonly known ***high-risk*** and ***medium-risk*** vulnerabilities. We also sought to assess the physical controls and environmental controls around critical information technology assets located in the NVFEL. We conducted this audit as part of the annual review of EPA's information security program as required by the Federal Information Security Management Act.

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

- *Strengthening 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/2012/20120927-12-P-0900.pdf

Results of Technical Network Vulnerability Assessment: EPA's National Vehicle and Fuel Emissions Laboratory

What We Found

While our assessments of EPA's NVFEL server room found no weaknesses with physical controls and environmental controls, vulnerability testing of networked resources located in the NVFEL identified Internet Protocol addresses with potentially 9 ***critical-risk***, 70 ***high-risk,*** and 297 ***medium-risk*** vulnerabilities. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network. The laboratory and the Office of Environmental Information manage the resources located in NVFEL that contained these weaknesses. We found a discrepancy between the offices concerning responsibility for certain equipment located in the NVFEL. However, NVFEL provided documentation which placed ownership responsibility with the Office of Environmental Information and Customer Technology Solutions for the devices in question.

Recommendations and Agency Corrective Actions

We recommend that the Senior Information Official within the Office of Air and Radiation and the Office of Environmental Information:

- Provide the OIG a status update for every critical-risk, high-risk and medium-risk vulnerability identified by the technical scanning tool within 30 days of this report.
- 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 within 30 days of this report.
- Perform a technical vulnerability assessment test of assigned networked resources within 60 days to confirm completion of remediation activities.

We also recommend that the Senior Information Official within the Office of Environmental Information:

- Disconnect any networked resources without documented ownership responsibility.
- Complete an inventory of all Customer Technology Solutions equipment prior to implementation of EPA's new managed desktop support system.

Representatives from both offices acknowledged the existence of the vulnerabilities and stated they have begun developing corrective actions to address the risks related to these weaknesses. NVFEL reported it remediated all high-risk vulnerabilities under its responsibility prior to the issuance of this report.

The detailed testing results have already been provided to Agency representatives. Due to the sensitive nature of the report's technical findings, the technical details will not be made available to the public.

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

THE INSPECTOR GENERAL

September 27, 2012

MEMORANDUM

SUBJECT: Results of Technical Network Vulnerability Assessment:
EPA's National Vehicle and Fuel Emissions Laboratory
Report No. 12-P-0900

FROM: Arthur A. Elkins, Jr.

TO: Betsy Shaw
Senior Information Official
Office of Air and Radiation

Renee Wynn
Principal Deputy Assistant Administrator and Senior Information Official
Office of Environmental Information

This is our quick reaction report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). Due to the sensitive nature of the technical findings, we are issuing this report for urgent management remediation. The site assessment was conducted in conjunction with our annual audit of EPA's information security program as required by the Federal Information Security Management Act. This report provides the summary of our security assessment of networked resources located at EPA's National Vehicle and Fuel Emissions Laboratory (NVFEL) in Ann Arbor, Michigan.

Our tests disclosed that networked resources at NVFEL contained potentially 9 ***critical-risk***, 70 ***high-risk,*** and 297 ***medium-risk*** vulnerabilities. The laboratory and Office of Environmental Information (OEI) are responsible for managing resources located in NVFEL. To facilitate immediate remediation actions, we provided your offices' representatives with the technical results during our site visit. Upon receipt of the results, NVFEL representatives identified OEI owned devices located on site. After providing OEI with a list of these devices, OEI stated that some of the devices were not under its responsibility. However, NVFEL provided documentation which placed ownership responsibility with OEI and Customer Technology Solutions for the devices in question. Ultimately, NVFEL representatives plan to take responsibility for remediating the vulnerabilities existing on the OEI devices in dispute. The NVFEL reported that it remediated all high-risk vulnerabilities under its responsibility prior to the issuance of this report.

We reported similar concerns about computer equipment accountability in EPA OIG Report No. 11-P-0705, *EPA's Contract Oversight and Controls Over Personal Computers Need Improvement,* September 26, 2011. Discrepancies in ownership responsibilities of networked resources can potentially lead to untimely vulnerability remediation or unresolved vulnerabilities that could expose EPA's assets to unauthorized access and potentially harm the Agency's network. As EPA moves from Customer Technology Solutions to a new contract for its managed desktop support system, it is important to resolve any discrepancies resulting from accountability for EPA assets that may be included in this new contract.

We performed this audit work from February through September 2012 at EPA's NVFEL in Ann Arbor, Michigan. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

We conducted testing to identify the existence of commonly known vulnerabilities using a commercially available network vulnerability assessment tool recognized by the National Institute of Standards and Technology (NIST). We interviewed EPA personnel responsible for managing the networked resources located in NVFEL. We reviewed relevant EPA interim procedures to obtain an understanding of the Agency's Automated Security Self-Evaluation and Remediation Tracking system used for recording identified weaknesses. We tested the Internet Protocol addresses associated with networked resources located in NVFEL. We used the risk ratings provided by the vulnerability software to determine the level of harm a risk could pose to a networked resource due to the vulnerability and accepted the results from the software tool as the level of risk to EPA's network. Upon follow-up with your offices' representatives, they acknowledged the existence of the vulnerabilities and stated that some mitigation activities had already begun related to these risks.

We performed an inspection of EPA's NVFEL server room with key information technology (IT) personnel to assess the physical controls and environmental controls around IT assets. We interviewed Agency IT staff to determine the extent to which IT equipment is protected from physical, environmental, and human threats. We used NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* as the template for evaluating IT security controls for the server rooms. We found no weaknesses during the assessment.

Recommendations

We recommend that the Senior Information Official within the Office of Air and Radiation and the Office of Environmental Information:

1. Provide the OIG a status update for every critical-risk, high-risk, and medium-risk vulnerability identified by the technical scanning tool within 30 days of this report.

2. 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 within 30 days of this report.

3. Perform a technical vulnerability assessment test of assigned networked resources within 60 days to confirm completion of remediation activities.

We also recommend that the Senior Information Official within the Office of Environmental Information:

4. Disconnect any networked resources without documented ownership responsibility.

5. Complete an inventory of all Customer Technology Solutions equipment prior to the implementation of EPA's new managed desktop support system.

Action Required

Please provide written responses to this report within 30 calendar days. You should include a corrective action plan for agreed-upon actions, including milestone dates.

Due to the sensitive nature of the report's technical findings, the technical details are not included in this report and will not be made available to the public. The OIG plans to post on the OIG's public website the corrective action plans that you provide to us that do not contain sensitive information. Therefore, we request that you provide the response to recommendation 1 in a separate document; we will not make that response available to the public if it contains sensitive information.

Your responses should be provided as Adobe PDF files that comply with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. Except for your response to recommendation 1, which will not be posted if it contains sensitive information, your responses should not contain data that you do not want to be released to the public; if those responses contain such data, you should identify the data for redaction or removal.

If you or your staff have any questions regarding this report, please contact Patricia H. Hill, Assistant Inspector General for Mission Systems, at (202) 566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard, Product Line Director, Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

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	2	Provide the OIG a status update for every critical-risk, high-risk, and medium-risk vulnerability identified by the technical scanning tool within 30 days of this report.	U	Senior Information Official, Office of Air and Radiation and Office of Environmental Information			
2	3	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 within 30 days of this report.	U	Senior Information Official, Office of Air and Radiation and Office of Environmental Information			
3	3	Perform a technical vulnerability assessment test of assigned networked resources within 60 days to confirm completion of remediation activities.	U	Senior Information Official, Office of Air and Radiation and Office of Environmental Information			
4	3	Disconnect any networked resources without documented ownership responsibility.	U	Senior Information Official, Office of Environmental Information			
5	3	Complete an inventory of all Customer Technology Solutions equipment prior to the implementation of EPA's new managed desktop support system.	U	Senior Information Official, Office of Environmental Information			

[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

Appendix A

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Assistant Administrator for Air and Radiation
Principal Deputy Assistant Administrator for Environmental Information and Senior Information Official
Senior Information Official, Office of Air and Radiation
Agency Follow-Up Official (the 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
Audit Follow-Up Coordinator, Office of Air and Radiation
Audit Follow-Up Coordinator, Office of Environmental Information