U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Results of Technical Network Vulnerability Assessment: EPA's Region 1

Report No. 12-P-0518 **June 5, 2012**

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

Report Contributors:

Rudolph M. Brevard
Warren Brooks
Scott Sammons
Kyle Denning

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-0518
June 5, 2012

At a Glance

Why We Did This Review

We sought to assess the security configurations of the U.S. Environmental Protection Agency's (EPA's) Region 1 wireless network infrastructure. We also sought to conduct network vulnerability testing of the Region 1 Local Area Network to identify resources that contained commonly known ***high-risk*** and ***medium-risk*** vulnerabilities.

Background

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. We conducted network vulnerability testing in February 2012 to identify any commonly known network vulnerabilities and to present the results to the appropriate EPA officials, who can then promptly remediate or document planned actions to resolve the weaknesses.

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/2012/20120605-12-P-0518.pdf

Results of Technical Network Vulnerability Assessment: EPA's Region 1

What We Found

Our vulnerability assessments of Region 1's wireless network infrastructure found no security weaknesses. However, our vulnerability testing of networked resources located at the Region 1 facility identified Internet Protocol addresses with potentially 18 ***high-risk*** and 166 ***medium-risk*** vulnerabilities. Regional and headquarter offices manage resources located in Region 1 that contain these weaknesses. The Office of Inspector General (OIG) met with EPA information security personnel from the respective offices to discuss the findings. EPA information security personnel acknowledged the existence of the identified security weaknesses and began immediate remediation of some of these issues. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

What We Recommend

We recommend that the Senior Information Officials within Region 1 and the Office of Environmental Information:

- Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings 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 network resources within 60 days to confirm completion of remediation activities.

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.

Planned Agency Corrective Actions

Region 1 remediated all high-risk vulnerabilities discovered by our vulnerability testing of networked resources. Additionally, Region 1 acknowledged the existence of the additional vulnerabilities that we identified and began mitigation activities related to these risks.

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

THE INSPECTOR GENERAL

June 5, 2012

MEMORANDUM

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

FROM: Arthur A. Elkins, Jr.

TO: Fred Weeks
Acting Senior Information Official
Region 1

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

This is our final report on the above subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). 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 testing of networked resources located at EPA's Region 1 office. Our test disclosed that network resources at the Region 1 office contained potentially 18 ***high-risk*** and 166 ***medium-risk*** vulnerabilities. Upon analysis of the testing results, we found that both regional and headquarters offices are responsible for managing the resources located in Region 1 that contain these weaknesses. We provided your office representatives with the technical results during our site visit in order to facilitate immediate remediation actions. All 18 high-risk vulnerabilities were remediated before the issuance of this report.

We performed this audit work from February through May 2012 at EPA's Region 1 offices in Boston, Massachusetts. We performed this audit in accordance with generally accepted government auditing standards. These 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. We interviewed EPA personnel responsible for managing the network resources located in Region 1. We reviewed relevant EPA policies to obtain an understanding of the Agency's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) system used for recording identified weaknesses. We tested the Internet Protocol addresses associated with network resources located in the Region 1 office. We used the risk ratings provided by the vulnerability software to determine the level of harm a vulnerability could cause to a networked resource and accepted the results from the software tool as the level of risk to EPA's network. Upon follow-up with your office representatives, they acknowledged the existence of the vulnerabilities and stated that some mitigation activities had already begun related to these risks.

We also conducted testing of Region 1's wireless infrastructure to identify any possible configuration weaknesses using a commercially available wireless scanning tool. Specifically, we tested to identify whether any unauthorized wireless devices existed on the region's network. We also tested to determine whether the wireless encryption protocols being used on the region's wireless local area network were sufficient to secure it. We found no weaknesses during either of these tests.

Recommendations

We recommend that the Senior Information Officials within Region 1 and the Office of Environmental Information:

1. Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings.

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.

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

Action Required

Please provide written responses to this report within 30 calendar days. You should include a corrective actions 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, and 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 all identified high-risk and medium-risk vulnerability findings.	U	Senior Information Officials, Region 1 and the Office of Environmental Information			
2	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.	U	Senior Information Officials, Region 1 and the Office of Environmental Information			
3	2	Perform a technical vulnerability assessment test of assigned network resources within 60 days to confirm completion of remediation activities.	U	Senior Information Officials, Region 1 and the 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
Regional Administrator, Region 1
Principal Deputy Assistant Administrator for Environmental Information and Senior Information Official
Acting Senior Information Official, Region 1
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 Environmental Information
Audit Follow-Up Coordinator, Region 1