U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Results of Technical Network Vulnerability Assessment: EPA's Region 6

Report No. 12-P-0659 **August 10, 2012**

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

Report Contributors: Rudolph M. Brevard
Warren Brooks
Scott Sammons
Jeremy Sigel

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-0659
August 10, 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 6 wireless network infrastructure. We sought to conduct network vulnerability testing of the Region 6 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 Region 6. 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.

Furthering EPA's Goals and Cross-Cutting Strategies

- *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/2012/20120810-12-P-0659.pdf

Results of Technical Network Vulnerability Assessment: EPA's Region 6

What We Found

Our vulnerability assessments of EPA's Region 6 wireless network infrastructure found no security weaknesses. However, our vulnerability testing of networked resources located at Region 6 facilities identified Internet Protocol addresses with potentially 35 ***critical-risk***, 217 ***high-risk,*** and 878 ***medium-risk*** vulnerabilities. Additionally, our server room assessments revealed a lack of adequate monitoring of environmental controls, the lack of a process to ensure only authorized personnel are approved for access to server rooms, and the existence of unsecured and unlogged media in the server rooms. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

Recommendations and Agency Corrective Actions

We recommend that the Senior Information Official within Region 6 provide the Office of Inspector General a status update for every critical-risk, high-risk, and medium-risk vulnerability identified by the scanning tool; create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities according to Agency interim procedures; perform a technical vulnerability assessment test of assigned network resources within 60 days to confirm completion of remediation activities; and remediate all identified physical and environmental control weaknesses identified in the server rooms.

Region 6 representatives acknowledged the existence of the vulnerabilities that we identified and stated they have begun developing corrective actions to address the risks related to these weaknesses.

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

August 10, 2012

MEMORANDUM

SUBJECT: Results of Technical Network Vulnerability Assessment:
EPA's Region 6
Report No. 12-P-0659

FROM: Arthur A. Elkins, Jr. Charles Sheehan for

TO: Lynda Carroll
Senior Information Official
Region 6

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 assessments were 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 assessments of networked resources located at EPA's Region 6 office in Dallas, Texas, and laboratory in Houston, Texas.

Our tests disclosed that network resources at the Region 6 office and laboratory contained potentially a combined 35 ***critical-risk***, 217 ***high-risk,*** and 878 ***medium-risk*** vulnerabilities. Our server room assessments revealed a lack of adequate monitoring of environmental controls, the lack of a process to ensure only authorized personnel are approved for access to server rooms, and the existence of unsecured and/or unlogged media in the server rooms. We provided your office representatives with the technical results during our site visit to facilitate immediate remediation actions.

We performed this audit work from February through August 2012 at EPA's Region 6 office in Dallas and laboratory in Houston. 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 network resources located in Region 6. 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 network resources located in the Region 6 office and laboratory. 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 office 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 Region 6 server rooms 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 around the server rooms. Appendix A includes a summary of our findings at the server rooms assessed and our recommendations by site.

We also conducted testing of EPA's Region 6 wireless infrastructure to identify any possible configuration weaknesses using a commercially available wireless scanning tool. Specifically, we performed tests to identify whether any unauthorized wireless devices existed on the region's network. We also performed tests 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 Official within Region 6:

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

4. Establish written procedures for granting authorized access to Region 6 server rooms in Dallas and Houston.

5. Sanitize and secure all used drives kept in the Houston server room in addition to logging their receipt, rotation, and/or disposal.

6. Establish a process for continuous monitoring of Dallas and Houston server rooms' environmental conditions by personnel or real-time monitoring by existing IT equipment with environmental monitoring capabilities.

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; 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 critical-risk, high-risk, and medium-risk vulnerability findings from the technical scanning tool within 30 days of this report.	U	Senior Information Official, Region 6			
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 within 30 days of this report.	U	Senior Information Official, Region 6			
3	2	Perform a technical vulnerability assessment test of assigned network resources within 60 days to confirm completion of remediation activities.	U	Senior Information Official, Region 6			
4	2	Establish written procedures for granting authorized access to Region 6 server rooms in Dallas and Houston.	U	Senior Information Official, Region 6			
5	3	Sanitize and secure all used drives kept in the Houston server room in addition to logging their receipt, rotation, and/or disposal.	U	Senior Information Official, Region 6			
6	3	Establish a process for continuous monitoring of Dallas and Houston server rooms' environmental conditions by personnel or real-time monitoring by existing IT equipment with environmental monitoring capabilities.	U	Senior Information Official, Region 6			

[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

Table of Server Room Assessment Findings and Recommendations by Site

Key: X = Weakness found at location

Issue Reviewed	Recommendations	Houston	Dallas
Lack of written procedures for authorizing access to the server rooms.	Establish written procedures for granting authorized access to Region 6 server rooms in Dallas and Houston.	X	X
Lack of environmental controls to monitor server room temperature and humidity and alert personnel of emergency.	Establish a process for continuous monitoring of Dallas and Houston server room's environmental conditions by personnel or real-time monitoring by existing IT equipment with environmental monitoring capabilities.	X	X
Charged wet-piped fire suppression system leaves uncovered server racks susceptible to water damage.		X	
Un-sanitized data drives with EPA information not logged and left unsecured within server room.	Sanitize and secure all used drives kept in the Houston server room in addition to logging their receipt, rotation and/or disposal.	X	
No logging of rotation of backup tapes or transportation/receipt at the Addison offsite storage facility.			X

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Regional Administrator, Region 6
Senior Information Official, Region 6
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, Region 6