



U.S. ENVIRONMENTAL PROTECTION AGENCY  
OFFICE OF INSPECTOR GENERAL

*Catalyst for Improving the Environment*

## Quick Reaction Report

# Results of Technical Network Vulnerability Assessment: EPA's Ronald Reagan Building

Report No. 10-P-0212

September 7, 2010

**Report Contributors:**

Rudolph M. Brevard  
Charles Dade  
Cheryl Reid  
Michael Goode, Jr.  
Vincent Campbell



# At a Glance

*Catalyst for Improving the Environment*

## Why We Did This Review

As part of the annual audit of the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Management Act, the Office of Inspector General (OIG) conducted network vulnerability testing of the Agency's network devices in EPA's Ronald Reagan Building located in Washington, DC.

## Background

Network vulnerability testing was conducted to identify any network risk vulnerabilities and to present the results to the appropriate EPA officials, who can then promptly remediate or document planned actions to resolve the vulnerability.

For further information, contact our Office of Congressional, Public Affairs and Management at (202) 566-2391.

To view the full report, click on the following link:  
[www.epa.gov/oig/reports/2010/20100907-10-P-0212.pdf](http://www.epa.gov/oig/reports/2010/20100907-10-P-0212.pdf)

## **Results of Technical Network Vulnerability Assessment: EPA's Ronald Reagan Building**

### What We Found

Vulnerability testing of EPA's Ronald Reagan Building network conducted in June 2010 identified Internet Protocol addresses with numerous *high-risk* and *medium-risk* vulnerabilities. The OIG met with EPA information security personnel to discuss the findings. 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 Director, Enterprise Desktop Solutions Division, Office of Environmental Information:

- Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings contained in this report.
- Create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities that cannot be corrected 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.

Due to the sensitive nature of the report's technical findings, the attachments are not available to the public.



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

THE INSPECTOR GENERAL

September 7, 2010

**MEMORANDUM**

**SUBJECT:** Results of Technical Network Vulnerability Assessment:  
EPA's Ronald Reagan Building  
Report No. 10-P-0212

**FROM:** Arthur A. Elkins, Jr.  
Inspector General

A handwritten signature in black ink, appearing to read "Arthur A. Elkins, Jr.", is written over the typed name.

**TO:** Johnny Davis, Jr.  
Director, Enterprise Desktop Solutions Division  
Office of Environmental Information

Attached is the final technical network vulnerability assessment report prepared by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA).<sup>1</sup> The site assessment was conducted in conjunction with the Fiscal Year 2010 Federal Information Security Management Act audit. Vulnerability testing of EPA's Ronald Reagan Building network conducted in June 2010 identified Internet Protocol addresses with numerous **high-risk** and **medium-risk** vulnerabilities.

We performed this audit from May through August 2010 at EPA's Ronald Reagan Building in Washington, DC. 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 tested Internet Protocol addresses provided by Agency representatives and identified as being associated with network resources controlled by your office. We used the risk ratings provided by the vulnerability software to determine the

---

<sup>1</sup> A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a tested information system. A vulnerability assessment does not include a penetration test which would attempt to use the identified vulnerabilities to gain further access into the tested information system.

level of harm a vulnerability could cause to a network resource. We accepted the results from the software tool. The vulnerabilities identified by the software are disclosed in the attachments.

The estimated cost for performing these tests and compiling this report is \$7,628.

## **Recommendations**

We recommend that the Director, Enterprise Desktop Solutions Division, Office of Environmental Information:

1. Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings contained in this report.
2. Create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities that cannot be corrected 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.

## **Action Required**

In accordance with EPA Manual 2750, you are required to provide a written response 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 full report will not be made available to the public. However, the OIG plans to publish the unrestricted version of this report, your response, and any corrective action plans on OIG's Website, which is available to the public. Therefore, we request that you provide your response to Recommendation 1 in a separate document.

If you or your staff have any questions regarding this report, please contact Rudy Brevard at (202) 566-0893 or [brevard.rudy@epa.gov](mailto:brevard.rudy@epa.gov).

# **Status of Recommendations and Potential Monetary Benefits**

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in \$000s)	
Rec. No.	Page No.	Subject	Status <sup>1</sup>	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 contained in this report.	U	Director, Enterprise Desktop Solutions Division, 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 that cannot be corrected within 30 days of this report.	U	Director, Enterprise Desktop Solutions Division, 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	Director, Enterprise Desktop Solutions Division, Office of Environmental Information			

<sup>1</sup> O = recommendation is open with agreed-to corrective actions pending  
 C = recommendation is closed with all agreed-to actions completed  
 U = recommendation is undecided with resolution efforts in progress

**Appendix A**

***Distribution***

Office of the Administrator  
Assistant Administrator for Environmental Information and Chief Information Officer  
Director, Enterprise Desktop Solutions Division, Office of Environmental Information  
Acting Senior Agency Information Security Officer  
Acting Director, Technology and Information Security Staff  
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  
Audit Follow-up Coordinator, Office of Environmental Information  
Inspector General