



U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

EPA's Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Room Security Controls

Report No. 12-P-0879

September 26, 2012



Scan this code to
learn more about
the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Michael Goode
Sabrena Stewart

Abbreviations

EPA	U.S. Environmental Protection Agency
IT	Information technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
NIST	National Institute of Standards and Technology
SP	Special Publication

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



At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to assess the security posture and in-place environmental controls of the computer rooms in the EPA Ariel Rios and Potomac Yard buildings in Washington, DC, and Arlington, Virginia, respectively. This audit was conducted in support of the audit of EPA's directory service system authentication and authorization servers.

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/2012/20120926-12-P-0879.pdf

EPA's Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Room Security Controls

What We Found

The security posture and in-place environmental control review of the computer rooms in the Ariel Rios and Potomac Yard buildings revealed numerous security and environmental control deficiencies. These control deficiencies greatly reduce the ability of the Office of Environmental Information (OEI) to safeguard critical information technology assets and associated data from the risk of damage and/or loss.

Recommendations/Planned Agency Corrective Actions

We recommended in our draft report that OEI remediate physical and environmental control deficiencies. Following the issuance of the draft report, OEI provided a corrective action plan with milestone dates to address agreed-upon recommendations. In its response, OEI agreed with recommendations 1 and 2, and stated that it had completed corrective actions for recommendation 1. OEI did not agree with recommendations 3 and 4 because it asserts that the Office of Administration and Resources Management bears responsibility for remediation for these recommendations. For recommendation 5, OEI did not agree because it stated that it is already monitoring environmental variable information which would alert it to the presence of a computer room water leakage. During the audit, the OIG requested policies and procedures that address limiting water damage to IT assets. OEI did not provide any documentation in response to this request and the OIG concluded that such policies did not exist.

We consider recommendation 1 closed with agreed-upon corrective actions complete. Recommendation 2 is open with agreed-upon corrective actions pending. The OIG believes that OEI bears the responsibility for addressing recommendations 3, 4, and 5 because it is responsible for managing IT assets in the Ariel Rios and Potomac Yard computer rooms. We consider recommendations 3, 4, and 5 unresolved with resolution efforts in progress.




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

THE INSPECTOR GENERAL

September 26, 2012

MEMORANDUM

SUBJECT: EPA's Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Room Security Controls
Report No. 12-P-0879

FROM: Arthur A. Elkins, Jr. 

TO: Vaughn Noga
Director, Office of Technology Operations and Planning
Office of Environmental Information

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

Action Required

The Office of Environmental Information (OEI) agreed with recommendations 1 and 2 and provided corrective action plans. OEI did not agree with recommendations 3, 4, and 5. These recommendations remain unresolved with resolution efforts in progress. Therefore, in accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days. You should include a corrective action plan for recommendations 3, 4, and 5, including milestone dates. Your response will be posted on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal. We have no objections to the further release of this report to the public. We will post this report to our website at <http://www.epa.gov/oig>.

If you or your staff have any questions regarding this report, please contact Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893 or

brevard.rudy@epa.gov; or Michael Goode, Project Manager, at (202) 566-0354 or goode.michael@epa.gov.

Table of Contents

Purpose	1
Background	1
Scope and Methodology	1
Findings	1
Lack of Monitoring, Oversight, and Procedures Increases Risk of Unauthorized Computer Room Access.....	2
Uninterruptible Power Supply Lacks Ability to Automatically Shut Down Critical IT Assets.....	3
Lack of Key Environmental Controls Increases Risk of Water Damage to Critical IT Assets.....	3
Recommendations	4
Agency Comments and OIG Evaluation	5
Status of Recommendations and Potential Monetary Benefits	6

Appendices

A Agency Response to Draft Report	7
B Distribution	11

Purpose

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to assess the security posture and in-place environmental controls of EPA's Office of Environmental Information (OEI) Ariel Rios computer room in Washington, DC, and Potomac Yard computer room in Arlington, Virginia. This audit was conducted in support of the audit of EPA's directory service system authentication and authorization servers

Background

OEI supports the Agency's mission to protect public health and the environment by integrating quality environmental information to make it useful for informing decisions, improving management, documenting performance, and measuring success. The Ariel Rios and Potomac Yard computer rooms house information technology (IT) assets that are used for Agency user authentication and authorization, Internet connectivity, and data storage.

Scope and Methodology

We performed this audit from January 2011 through May 2012 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 our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We conducted the on-site review of the computer room security posture and in-place environmental controls at the Ariel Rios and Potomac Yard computer rooms in Washington, DC, and Arlington, Virginia, respectively, in April 2011. The criteria used for the review were derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, "Physical and Environmental Protection Security" control family. We evaluated the computer rooms through inquiry, observation, and review of documentation.

We had no prior report recommendations for follow up during this audit for these two specific sites.

Findings

The Ariel Rios and Potomac Yard computer room control deficiencies greatly reduce the ability of OEI to safeguard critical IT assets and associated data from the risk of unauthorized access, damage, and/or loss. In particular, physical access controls were not in place to monitor access to critical IT assets, and the server

room lacked environmental controls to protect these assets from potential loss or damage due to power outages and water leaks. NIST prescribes the selection and implementation of appropriate security controls for an information system, which represent the management, operational, and technical safeguards or countermeasures employed to protect the confidentiality, integrity, and availability of the system and its information. If OEI does not correct identified weaknesses, it faces potential disruption of its operations.

Lack of Monitoring, Oversight, and Procedures Increases Risk of Unauthorized Computer Room Access

The OIG was unable to determine if OEI has any policies and procedures in place to ensure that computer room access is only granted to authorized employees. The OIG was also unable to determine if OEI maintains a listing of employees authorized to access the computer room. OEI indicated that they randomly review the authorized employee access list, but the OIG was not provided with any documentation to support that assertion. OEI's Ariel Rios and Potomac Yard computer room visitor logs had not been used or reviewed. This lack of computer room access controls increases the risk that unauthorized individuals may gain entry into the computer room and damage critical IT assets.

NIST SP 800-53 states that an organization must do the following:

- Develop, disseminate, and review/update a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Develop and keep current a list of personnel with authorized access to the facility where the information system resides
- Review and approve the access list and authorization credentials, removing from the access list personnel no longer requiring access
- Maintain visitor access records to the facility where the information system resides
- Review visitor access records

OEI must establish physical access policies and procedures to ensure that access to facilities containing critical IT assets is documented and regularly reviewed by management. OEI must also utilize and review visitor access logs for computer rooms. These steps are essential to mitigating the risk of damage to critical IT assets.

Uninterruptible Power Supply Lacks Ability to Automatically Shut Down Critical IT Assets

In emergency situations, OEI has only a limited ability to shut down the Ariel Rios and Potomac Yard computer room IT assets in an orderly fashion. The possibility of an orderly shutdown is hindered by the following conditions:

- Lack of generator to provide emergency power
- Lack of around-the-clock staff presence in computer rooms
- Short duration of existing uninterruptible power supply to provide backup power
- Lack of uninterruptible power supply capable of automatically shutting down IT assets

NIST SP 800-53 states that an organization should provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

In the Potomac Yard computer room, authorized personnel have only 1 hour and 30 minutes from the time power is lost to get to the computer room and manually shut down the IT equipment; in the Ariel Rios computer room, we were told that the length of time is only 3 minutes. These short periods during which backup power is available, combined with the lack of dedicated around-the-clock staff manning the computer rooms and the lack of an emergency generator and automatic shutdown capabilities, increase the likelihood that personnel will not be able to perform an orderly shutdown of IT assets in the event of a power loss.

Lack of Key Environmental Controls Increases Risk of Water Damage to Critical IT Assets

Ariel Rios and Potomac Yard computer room IT assets are at risk of damage due to accidental water leakage. Server cabinets containing the IT assets are located directly under the computer rooms' overhead sprinklers, and the fire suppression systems within the rooms are fully charged. Fully charged fire suppression systems maintain water pressure at all times. These pipes could leak, especially at points where the sprinkler heads connect to the water pipes. The computer rooms also did not have compensating controls, such as leak shields, to protect these assets from potential water damage.

Where there is a fully charged fire suppression system, the risk of water damage from leaks may be mitigated by not placing IT assets directly under sprinkler heads or pipes when possible. When it is not possible to relocate IT assets to areas not directly under sprinkler heads and pipes, other compensating controls such as leak shields attached to or above the cabinets should be utilized.

The Ariel Rios and Potomac Yard computer rooms also did not have formal procedures related to monitoring for water leaks in the computer room or for actions to be taken in the event of a water leak. In addition, the Ariel Rios and Potomac Yard computer rooms did not have master shutoff valves for the water pipes running through the computer rooms or water detectors on the floor of the computer rooms to alert personnel and permit them to take timely action in the case of a water leak.

The U.S. Government Accountability Office *Federal Information System Controls Audit Manual* specifies that environmental controls exist to help ensure that building plumbing lines do not endanger the computer facility or, at a minimum, that shutoff valves and procedures exist and are known. NIST SP 800-53 stipulates that an organization should protect information systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Recommendations

We recommend that the Director, Office of Technology and Operations Planning, Office of Environmental Information:

1. Develop and implement computer room policies and procedures that ensure that computer room access is only grant to authorized employees and that visitor access is approved, documented, and reviewed.
2. Acquire and implement an uninterruptible power supply that will automatically perform an orderly shutdown of IT assets without manual intervention in the event of a long-term loss of power.
3. Move the server racks so that they are not directly under sprinkler heads or water pipes, or, if that is not possible, install leak shields on or above the server racks directly under sprinkler heads or water pipes.
4. Install a master shutoff valve for the water pipes that flow through the computer room.
5. Develop and implement policies and procedures that address limiting water damages to IT assets in the computer room that include:
 - a. 24 hours/day, 7 days/week monitoring
 - b. Timely actions to be taken in the event of a water leak in the computer room

Agency Comments and OIG Evaluation

Following the issuance of the draft report, OEI provided a corrective action plan with milestone dates to address agreed-upon recommendations. In its response, OEI agreed with recommendations 1 and 2, but did not agree with recommendations 3, 4, and 5. OEI did not agree with recommendations 3 and 4 because it asserts that the Office of Administration and Resources Management bears responsibility for remediation for these recommendations. For recommendation 5, OEI did not agree because it stated that it is already monitoring environmental variable information which would alert it to the presence of a computer room water leakage. OEI also stated that it has completed corrective actions for recommendation 1.

We consider recommendation 1 closed with agreed-upon corrective actions complete. Recommendation 2 is open with agreed-upon corrective actions pending. The OIG believes that OEI bears the responsibility for recommendations 3 and 4 because it is responsible for managing IT assets in the Ariel Rios and Potomac Yard computer rooms. Therefore, OEI needs to ensure that corrective actions are carried out for recommendations 3 and 4. During the audit, the OIG requested any policies and procedures that address limiting water damage to IT assets. OEI did not provide any documentation for this request and the OIG concluded that such policies did not exist. Therefore, recommendation 5 was made to OEI. We consider recommendations 3, 4, and 5 unresolved with resolution efforts in progress.

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	4	Develop and implement computer room policies and procedures that ensure that computer room access is only grant to authorized employees and that visitor access is approved, documented, and reviewed.	C	Director, Office of Technology and Operations Planning, Office of Environmental Information			
2	4	Acquire and implement an uninterruptible power supply that will automatically perform an orderly shutdown of IT assets without manual intervention in the event of a long-term loss of power.	O	Director, Office of Technology and Operations Planning, Office of Environmental Information			
3	4	Move the server racks so that they are not directly under sprinkler heads or water pipes, or, if that is not possible, install leak shields on or above the server racks directly under sprinkler heads or water pipes.	U	Director, Office of Technology and Operations Planning, Office of Environmental Information			
4	4	Install a master shutoff valve for the water pipes that flow through the computer room.	U	Director, Office of Technology and Operations Planning, Office of Environmental Information			
5	4	Develop and implement policies and procedures that address limiting water damages to IT assets in the computer room that include: a. 24 hours/day, 7 days/week monitoring b. Timely actions to be taken in the event of a water leak in the computer room	U	Director, Office of Technology and Operations Planning, 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

Agency Response to Draft Report

June 29, 2012

MEMORANDUM

SUBJECT: Follow-on Responses to Audit: *EPA's Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Room Security Controls*, Report Project No. OMS-FY11-0007

FROM: Maja Lee
Acting Director, Enterprise Desktop Solutions Division
Office of Technology Operations and Planning

THRU: Vaughn Noga,
Director, Office of Technology Operations and Planning and
Chief Technology Officer

TO: Rudolph M. Brevard
Director, Information Resources Management Assessments
Office of the Inspector General

The purpose of this memorandum is to provide a response to the subject draft report and provide additional clarification regarding the Office of Environmental Information's (OEI) security controls at the Ariel Rios and Potomac Yard Server Room facilities.

OEI appreciates the OIG's desire to ensure EPA has adequate security controls in place. Attached is a detailed response to the draft report and a Corrective Action Plan for the actions which the Office of Technology Operations and Planning (OTOP) has the lead.

If you have any questions regarding this response, please contact me at 202-566-0300.

Attachments

Cc: Anne Mangiafico
Maja Lee

**Office of Environmental Information
Corrective Action Plan
As of 07/11/12**

Auditing Group: OIG Audit No.: OMS-FY11-0007 Report Date: May 31, 2012 OEI Lead Office: OTOP/EDSD	Audit Title: Draft Report – EPA’s Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Rooms Security Controls OEI Lead and Phone: James Freeman 703-305-8186
--	---

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
1. Develop and implement computer room policies and procedures that ensure that computer room access is only granted to employees with authorization and that visitor access is approved, documented, and reviewed.		Completed Policies and procedures are currently in place to ensure that computer room access is only granted to employees with authorization and that visitor access is approved, documented and reviewed.		Memorandum title: Request for Access to Secure Areas (Data Center/LAN closet) creation date June 8,2011
2. Acquire and implement an uninterruptible power supply that will automatically perform an orderly shutdown of IT assets without manual intervention in the event of a long-term loss of power.		Concur As part of the Federal Government’s data consolidation initiative, the Ariel Rios computer room will be closed and the servers migrated to Potomac Yard. Efforts are underway with GSA to install a backup generator at the	Dec. 31, 2012	POAM’s will be created in ASSERT to track the installation of the new power source for Potomac Yard and the Federal Government data center consolidation initiative that will affect computer rooms at EPA headquarters.

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
		<p>Potomac Yard facility. The generator will provide 24/7 backup power to the computer room and in the event of a prolonged power outage, sufficient notification would enable an orderly shutdown of IT assets.</p>		
<p>3 Move the server racks so that they are not directly under sprinkler heads or water pipes, or, if that is not possible, install leak shields on or above the server racks directly under sprinkler heads or water pipes.</p>		<p>Non-Concur As part of the Federal Government's data consolidation initiative, the Ariel Rios computer room will be closed and the servers migrated to Potomac Yard. Water damage cannot be avoided if the sprinkler system is activated and operates per specifications (i.e. sprays water).</p> <p>Refer to OARM -</p>		

Recommendation	OIG Revised Recommendations	Corrective Action	Planned Completion Date	Status / Actions Taken
		OARM is responsible for the facility and water sprinklers.		
4. Install a master shutoff valve for the water pipes that flow through the computer room.		Non-Concur Refer to OARM - OARM is responsible for the facility, water pipes and shut off valves.		
5. Develop and implement policies and procedures that address limiting water damages to IT assets in the computer room that include a) 24 hours/day, 7 days/week monitoring; and (2) timely actions to be taken in the event of a water leak in the computer room.		Non-Concur Monitoring of environmental variable information such as water, fire, temperature, humidity, power, and smoke is part of the current standard procedures, is monitored 24/7 and issues are reported to an identified group by text message and email.		EPA monitors environmental variable information through HP Openview with e-mail and text message notifications to personnel in order to address any reported issues.

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Principal Deputy Assistant Administrator for Environmental Information
and Senior Information Official
Director, Office of Technology Operations and Planning, Office of Environmental Information
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, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Environmental Information