U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

EPA's Radiation and Indoor Environments National Laboratory Should Improve Its Computer Room Security Controls

Report No. 12-P-0847 **September 21, 2012**

Scan this mobile 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
NIST	National Institute of Standards and Technology
OAR	Office of Air and Radiation
OIG	Office of Inspector General
ORD	Office of Research and Development
RIENL	Radiation and Indoor Environments National Laboratory
SP	Special Publication

U.S. Environmental Protection Agency
Office of Inspector General

12-P-0847
September 21, 2012

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 EPA's Radiation and Indoor Environments National Laboratory computer room in Las Vegas, Nevada. 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/2012/20120921-12-P-0847.pdf

EPA's Radiation and Indoor Environments National Laboratory Should Improve Its Computer Room Security Controls

What We Found

Our review of the security posture and in-place environmental controls of EPA's Radiation and Indoor Environments National Laboratory computer room disclosed an array of security and environmental control deficiencies. These deficiencies greatly hinder the ability of the Office of Air and Radiation (OAR) to safeguard critical information technology assets and associated data from the risk of damage and/or loss.

Recommendations and Planned Agency Corrective Actions

We recommended in our draft report that OAR remediate physical and environmental control deficiencies. In its response to the draft report, OAR provided a corrective action plan with milestone dates to address agreed-upon recommendations 1 through 5. OAR did not agree or disagree with recommendation 6 because corrective actions required consultation with the U.S. General Services Administration to identify a suitable resolution.

OAR subsequently submitted an updated status on agreed-upon corrective actions. Based upon that status, corrective actions for recommendations 1 through 5 have been completed. In the updated status, OAR proposed an alternative action of accepting the risks of not installing the emergency shut-off valve for recommendation 6. OAR made this proposal because its initial investigation suggested that compliance would be cost prohibitive and the local fire code may make necessary modifications infeasible. OAR agreed to assume the risks associated with that decision.

We consider recommendations 1 through 5 closed with agreed-upon corrective actions complete. For recommendation 6, we accept OAR's proposal and have updated it to reflect necessary steps OAR must undertake to implement the proposed alternative action. Specifically, OAR management should update its information security plan to formally accept the risks for not meeting minimum information systems security controls required by federal guidance. OAR concurred with the update to recommendation 6. Although OAR has concurred with the recommendation change, we consider recommendation 6 unresolved pending receipt of a corrective action plan with milestone completion dates.

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

THE INSPECTOR GENERAL

September 21, 2012

MEMORANDUM

SUBJECT: EPA's Radiation and Indoor Environments National Laboratory Should Improve Its Computer Room Security Controls
Report No. 12-P-0847

FROM: Arthur A. Elkins, Jr.

TO: Jim Jones
Senior Information Official
Office of Air and Radiation

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 Air and Radiation (OAR) provided an acceptable corrective action plan and has completed agreed-upon corrective actions for recommendations 1 through 5. In OAR's response to the draft report, it neither agreed nor disagreed with recommendation 6. Subsequently, OAR proposed an alternative action to resolve recommendation 6. The OIG accepts OAR's proposed alternative action and has updated recommendation 6 to reflect necessary steps OAR must undertake to implement the proposed alternative action. However, we consider recommendation 6 unresolved pending receipt of a corrective action plan with milestone completion dates.

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 recommendation 6, 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

Appendices

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 Radiation and Indoor Environments National Laboratory (RIENL) computer room in Las Vegas, Nevada. This audit was conducted in support of the audit of EPA's directory service system authentication and authorization servers.

Background

The RIENL protects the public and the environment by minimizing public exposure to radiation and indoor air pollution through environmental measurements, applied technologies, and education. The laboratory also provides scientific and technical support for the Agency's radiation, ambient air quality, and indoor environments programs at EPA headquarters and in the regions; other federal agencies; tribal, state, and local governments; and private industry. The laboratory is part of the Office of Air and Radiation (OAR).

Scope and Methodology

We performed this audit from January 2011 through April 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 RIENL in Las Vegas, Nevada, in March 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 RIENL computer room through inquiry, observation, and review of documentation. At the time of our visit in March 2011, we met with OAR representatives and shared our findings with them. While onsite for another audit in September 2011, we met with OAR representatives to determine whether the findings we identified in March 2011 had been remediated.

Prior OIG Reports

In EPA OIG Report No. 10-P-0059, *EPA Needs to Improve Physical Security at Its Offices in Las Vegas, Nevada*, February 3, 2010 (2010 Report), we found that the Office of Research and Development (ORD) operated the access control system for EPA's Las Vegas offices, and granted personnel access to sensitive

areas without proper authorization. We recommended that ORD develop and implement procedures to ensure that all organizations are provided with the information necessary to monitor and review the access to their space until offices accept the responsibility from ORD. We also recommended that the Office of Administration and Resources Management's Security Management Division conduct an assessment of the physical security practices at EPA's Las Vegas locations and conduct outreach to the Las Vegas offices to provide assistance. EPA agreed with the findings and recommendations.

Findings

RIENL computer room control deficiencies greatly reduce the ability of OAR 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. Also, the server room lacked environmental controls to protect IT 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. Although OAR has taken steps to correct some of the weaknesses noted during our initial site visit in March 2011, additional steps are needed. We believe that OAR faces potential disruption of its operations if it does not correct the identified weaknesses.

Computer Room Servers Unsecured and Without Compensating Controls

In March 2011, we found that critical servers in the RIENL computer room were not secured in locked cabinets to prevent unauthorized access. NIST SP 800-53 specifies that organizations should use lockable physical casings to protect information system components from unauthorized physical access. We noted that the cabinets were not locked because the rack-mounted IT assets exceeded the length of the server cabinets, thereby preventing the cabinets from being locked without potentially damaging the IT assets.

Additionally, management had not implemented compensating controls such as video monitoring of the computer room to ensure the capability of identifying the cause of a service disruption or to serve as a reference point to plan risk mitigation procedures. NIST SP 800-53 recommends that organizations guard, alarm, and monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week. The computer room is controlled by a card access system. However, in our 2010 Report, we had noted weaknesses within the card access system. As a result of this previously identified weakness and issues identified during this audit, the OIG believes that video cameras are an additional safeguard that will aid in monitoring personnel activity.

We shared these findings with OAR representatives in March 2011. We also met with OAR representatives in September 2011 to determine whether the office took steps to address these weaknesses. During our subsequent walkthrough, we noted that OAR had installed four new server cabinets to correct the previously identified issue associated with the rack-mounted IT assets. All rack-mounted IT assets now properly fit into the server cabinets. However, not all server cabinet doors were locked. The unlocked server cabinet doors leave the servers and associated IT assets vulnerable to unauthorized access, tampering, and/or theft.

Additionally, while conducting the September 2011 visit, we noted that a video camera had been installed on the wall of the computer room. This camera appears to monitor computer room entry/exit points and the server cabinets. This video is monitored and recorded outside of the computer room. However, OAR representatives could not provide us with any policies and/or procedures that outline monitoring practices and responsibilities. NIST SP 800-53 specifies that organizations should document physical and environmental protection procedures that address purpose, scope, roles, and responsibilities. We could not test the new video surveillance system because personnel responsible for the video surveillance system were not available during our visit.

No Automatic Shutdown Capabilities for Power System

In emergency situations, RIENL's ability to shut down IT equipment in an orderly fashion is limited. 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. The possibility of an orderly emergency shutdown is hindered by the lack of (1) a generator to provide emergency power, (2) around-the-clock monitoring of the RIENL computer room, and (3) an uninterruptible power supply with automated shutdown capability.

OAR personnel indicated that once power is lost, its uninterrupted power supply only provides 20 minutes of backup power to manually shut down IT equipment. This short period during which back-up power is available, combined with the lack of dedicated around-the-clock staff manning the computer room and the lack of automatic shutdown capabilities, increases the likelihood that personnel will not be able to perform an orderly shutdown of IT assets in the event of a power loss. Inability to perform an orderly shutdown increases the risk of data loss.

Servers Exposed to Potential Water Damage

RIENL IT assets are at risk of damage due to accidental water leakage. 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. The manual also points to the need for water detectors on the floor of the facility. 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. Server cabinets containing the IT assets were located directly under the computer room's overhead sprinklers, and the fire suppression system within the room is fully charged. Fully charged fire suppression systems maintain water pressure at all times, and these pipes could leak, especially at points where the sprinkler heads connect to the water pipes. The computer room also did not have compensating controls, such as leak shields, to protect these assets from potential water damage.

When organizations have a fully charged fire suppression system, the risk of water damage from leaks may be mitigated by removing IT assets from areas 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.

OAR does not have formal procedures related to monitoring potential water leaks in the computer room, or for actions to be taken in the event of a water leak. In addition, the computer room does not have a master shutoff valve for the water pipes running through the computer room.

Recommendations

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

1. Develop and implement computer room policies and procedures to ensure that server cabinets are locked at all times, except when IT assets are being worked on.

2. Develop and implement computer room policies and procedures related to video surveillance of the physical access to critical assets within the computer room including, but not limited to, detailed procedures that specify:

    a. How long video footage should be maintained
    b. How video surveillance reviews should be performed
    c. How often video footage should be reviewed
    d. The groups and persons responsible for reviewing video surveillance footage

3. Develop and implement computer room policies and procedures to limit water damage to the IT assets in the computer room, to 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

4. Acquire and implement an uninterrupted 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.

5. 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.

6. Install a master shutoff valve for the water pipes that flow through the computer room or update the local area network security plan to have the Authorizing Official formally accept the risks of operating the facility without installing the valve.

Agency Comments and OIG Evaluation

OAR responded to our draft report and provided a corrective action plan with milestone dates to address agreed-upon recommendations 1 through 5. OAR did not agree or disagree with recommendation 6. Corrective actions for this recommendation required consultation with the U.S. General Services Administration because that office leases the OAR facility under review. This response is provided in Appendix A.

OAR subsequently submitted an updated status on agreed-upon corrective actions. Based upon the OIG review of the updated status of corrective actions and supporting documentation, we consider recommendations 1 through 5 closed and associated corrective actions complete. In the updated status, OAR proposed an alternative action of accepting the risks associated with not installing the emergency shut-off valve for recommendation 6. OAR made this proposal because its initial investigation suggested that compliance would be cost prohibitive and the local fire code may make modifications infeasible.

We accept OAR's proposal regarding recommendation 6 and have updated it to reflect necessary steps OAR must undertake to implement the proposed alternative action. Specifically, OAR management should update its information security plan to formally accept the risks of not installing the emergency shut-off valve as specified by NIST 800-53. OAR concurred with the update to recommendation 6. Although OAR has concurred with the recommendation change, we consider recommendation 6 unresolved pending receipt of a corrective action plan with milestone completion dates.

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 to ensure that server cabinets are locked at all times, except when IT assets are being worked on.	C	Senior Information Official, Office of Air and Radiation			
2	4	Develop and implement computer room policies and procedures related to video surveillance of the physical access to critical assets within the computer room including, but not limited to, detailed procedures that specify: a. How long video footage should be maintained b. How video surveillance reviews should be performed c. How often video footage should be reviewed d. The groups and persons responsible for reviewing video surveillance footage	C	Senior Information Official, Office of Air and Radiation			
3	4	Develop and implement policies and procedures to limit water damage to the IT assets in the computer room, to 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	C	Senior Information Official, Office of Air and Radiation			
4	5	Acquire and implement an uninterrupted 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.	C	Senior Information Official, Office of Air and Radiation			
5	5	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.	C	Senior Information Official, Office of Air and Radiation			
6	5	Install a master shutoff valve for the water pipes that flow through the computer room or update the local area network security plan to have the Authorizing Official formally accept the risks of operating the facility without installing the valve.	U	Senior Information Official, Office of Air and Radiation			

[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

Agency Response to Draft Report

MEMORANDUM

SUBJECT: Response to Recommendations for Improving EPA's Radiation and Indoor Environments National Laboratory (R&IENL) Computer Room Security Controls - Project No. OMS-FY11-0009

FROM: Elizabeth Shaw
Acting Deputy Assistant Administrator

TO: Rudolph M. Brevard
Director, Information Resources Management Assessments

This document outlines solutions in concurrence to recommendations made in the OIG report, dated April 26, 2012, stating security controls at R&IENL need improvement.

OIG recommendation # 1: Develop and implement computer room policies and procedures to insure that server cabinets are locked at all times, except when IT assets are being worked on and regular maintenance performed.

OAR Response: In concurrence with the above recommendation, a memorandum outlining current R&IE computer server room security policies and procedures is in development. As noted in the OIG report, R&IE IT personnel were aware of the issue and working on a remediation strategy prior/during/after the IG inspection. Server rack replacement cost and time for completion has taken over one year.

Planned Completion Date:
June 29, 2012

OIG recommendation # 2: Develop and implement computer room policies and procedures related to video surveillance of the physical access to critical assets within the computer room including, but not limited to, detailed procedures that specify:
a. How long video footage should be maintained
b. How and when video surveillance reviews should be performed
c. How often video footage should be reviewed
d. The groups and persons responsible for reviewing video surveillance footage

OAR Response: In concurrence with the above recommendation, a CCTV SOP is in development to address policies and procedures related to the La Plaza CCTV system. This system resides in the R&IE GSS and is jointly managed with OCFO/LVFC providing services to all seven AA offices at the La Plaza Business Center. OAR/ORIA/RIE will work with OCFO/LVFC management and IT staff in order to meet this recommendation.

Planned Completion Date:
July 31, 2012

OIG recommendation # 3: Develop and implement policies and procedures to limit water damage to the IT assets in the computer room, to include:
a. 24 hours/day, 7 days/week monitoring
b. Timely actions to be taken in the event of water leak in the computer room

OAR Response: In concurrence with the above recommendation, a memorandum outlining current R&IE's Server Room Environmental System Control policies and procedures will be developed. This memo will outline environmental controls currently available in the server room such as water, heat, and noise alerts and our automated 24/7 monitoring system.

Planned Completion Date:
June 29, 2012

OIG recommendation # 4: Acquire and implement an uninterrupted power supply (UPS) that will automatically perform an orderly shutdown of IT assets without manual intervention in the event of a long-term loss of power.

OAR Response: In concurrence with the above recommendation, a software and hardware solution has been researched to implement an orderly shutdown on all compatible systems. Recently the primary server environment was migrated to a VM system. Prior to this migration, due to the age of our servers, it was not possible to properly and efficiently implement this recommendation.

Planned Completion Date:
August 31, 2012

OIG recommendation # 5: 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.

OAR Response: In concurrence with the above recommendation, a sheet metal contractor has been contracted to design, construct and install water leak shields on all five server racks that are directly under sprinkler heads and water pipes.

Planned Completion Date:
August 31, 2012

OIG recommendation # 6: Install a master shutoff valve for the water pipes that flow through the computer room.

OAR Response: R&IE server room is located in a space leased by GSA. Further research needs to be conducted by GSA in order to establish whether this recommendation is feasible for implementation or if cost is prohibitive. Preliminary R&IE research indicates local city/county fire department policies may make this infeasible based on the current building infrastructure.

Planned Completion Date:
TBD

cc: Larry Dollison
Mike Flynn
Ron Fraass
Reginald Slade
Maureen Hingeley

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Air and Radiation
Deputy Assistant Administrator for Air and Radiation
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
Director, Radiation and Indoor Environments National Laboratory, Office of Air and Radiation
Audit Follow-Up Coordinator, Office of Air and Radiation
Information Security Officer, Office of Air and Radiation