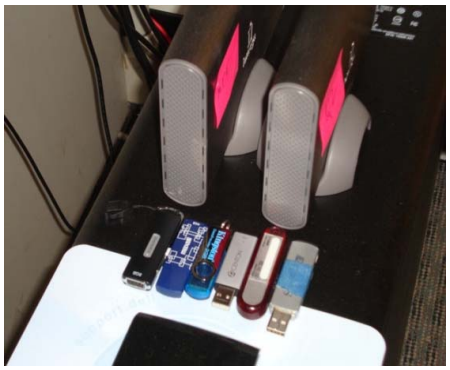
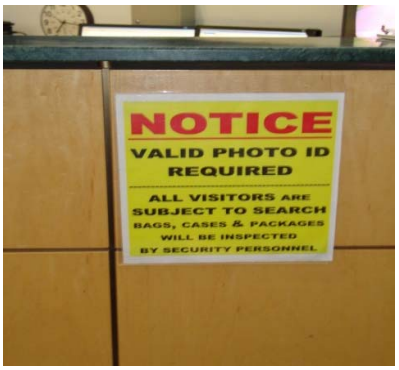
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities

Report No. 13-P-0252 **May 8, 2013**





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

Report Contributors:

Rudolph M. Brevard
Warren Brooks
Teresa Richardson
Jeremy Sigel
Eric Jackson
Kyle Denning

Abbreviations

AED	Atlantic Ecology Division
CCTV	Closed-circuit television
COOP	Continuity of operations
ERD	Ecosystems Research Division
EPA	U.S. Environmental Protection Agency
GED	Gulf Ecology Division
IT	Information technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORD	Office of Research and Development
PCs	Personal computers
SP	Special Publication
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

Cover photos: *Clockwise from top left:* Unsecured thumb drives; signage at entrance; Gulf Ecology Division buildings. (EPA OIG photos)

U.S. Environmental Protection Agency
Office of Inspector General

13-P-0252
May 8, 2013

At a Glance

Why We Did This Review

We sought to determine to what extent management at U.S. Environmental Protection Agency-owned research facilities establish and implement information security practices to protect Agency information technology assets. Agency IT assets must be maintained in accordance with security requirements defined by applicable federal laws, executive orders, directives, policies, standards, and regulations to ensure adequate confidentiality, availability, and integrity of the resources and information stored on or transmitted through the EPA network. Network vulnerabilities can expose IT assets to significant risk and disrupt operations if not identified and resolved.

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/2013/20130508-13-P-0252.pdf

Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities

What We Found

Facilities management at the Office of Research and Development facilities does not consistently apply, or in some cases establish, controls to protect IT assets. We found instances where IT security practices at the facilities did not meet minimal recommended controls for securing IT assets. Chief among our findings are the following:

- IT equipment was unprotected from and unmonitored for water damage.
- Access to server rooms was unrestricted.
- No continuity of operations plan exists for provisioning IT equipment.
- Backup data were not stored offsite.

The National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* among other federal and Agency policies and procedures, provides minimum security-control recommendations. Many security weaknesses occurred at ORD facilities because these facilities did not follow federal and Agency guidance that prescribes measures for securing IT assets. Further, ORD facilities did not consistently perform or, when necessary, enhance security practices established to protect their facilities, as well as the IT resources within their custody. Failure to consistently follow, perform, and monitor recommended and established security practices compromises the security of IT assets, disrupts business operations, and exposes sensitive Agency information.

Recommendations and Planned Agency Corrective Actions

Management agreed with 14 of the 18 report recommendations to improve practices at ORD facilities. We consider these recommendations unresolved until the Agency provides planned completion dates. Management did not agree with recommendations to improve controls around the closed-circuit television system and to protect servers from accidental water damage. These recommendations are unresolved. We believe it is incumbent upon management to assess the risks for not implementing these needed measures. Furthermore, when required by federal guidance, management should document its decisions and have the responsible official formally accept responsibility.

Noteworthy Achievements

We conducted tests to determine the effectiveness of security practices for remote-access capability. We concluded that ORD labs implemented effective IT security controls that prevent unauthorized connection and communication by limiting access to the Agency's network through wireless network-access points.

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

THE INSPECTOR GENERAL

May 8, 2013

MEMORANDUM

SUBJECT: Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities
Report No. 13-P-0252

FROM: Arthur A. Elkins Jr.

TO: Lek Kadeli, Principal Deputy Assistant Administrator
Office of Research and Development

This is our report on the subject audit conducted by the Office of Inspector General of the U.S. Environmental Protection Agency. 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. EPA agreed with 14 of the recommendations. However, we consider these recommendations unresolved until ORD provides estimated completion dates. The Agency and the OIG disagreed on the other four recommendations and these will be addressed through the audit resolution process. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, the resolution process begins immediately with the issuance of this report. We are requesting a meeting within 30 days between the Deputy Assistant Administrator for Management for the Office of Research and Development and the OIG's Assistant Inspector General for the Office of Audit to resolve the four recommendations to which ORD disagrees. During the 30 days, we are requesting the planned completion dates for the remaining 14 recommendations. If resolution is still not reached, the ORD is required to complete and submit the dispute resolution request to the Chief Financial Officer to continue resolution.

If you or your staff have any questions regarding this report, please contact Richard Eyermann, Acting Assistant Inspector General for the Office of Audit, at (202) 566-0565 or eyermann.richard@epa.gov; or Rudolph M. Brevard, Director of Information Resources Management Audits, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Chapters

-continued-

Appendices

Chapter 1
Introduction

Purpose

We sought to determine to what extent management at U.S. Environmental Protection Agency research facilities establish and implement security practices to protect Agency information technology assets.

Background

IT assets require countermeasures and security controls that protect computer-processing capabilities and mitigate the risk of loss caused by theft, fire, flood, intentional destruction and damage, mechanical equipment and power failures, and unauthorized access. Security controls are the management, operational, and technical safeguards employed in an information system to protect the confidentiality, integrity, and availability of the system and its information. Without protective countermeasures and security controls applied to information systems, Agency operations could be disrupted.

Noteworthy Achievements

For each of the sites visited, we conducted tests to determine the effectiveness of security practices for remote-access capability. Remote access is the ability to communicate with another computer or network over communication lines. From our tests, we concluded that Office of Research and Development labs implemented effective IT security controls that prevent unauthorized connection and communication by limiting access to the Agency's network through wireless network-access points.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, 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 this audit from February 2011 through October 2012. We evaluated the EPA's controls designed to protect IT assets from physical, environmental, and human threats. We focused on facilities that the EPA owns and therefore has sole responsibility for the security of IT assets. We further

limited our selection to program offices that occupy the majority of these facilities.

ORD labs are the primary occupants for 12 of the 21 EPA-owned facilities. From this group of 12 facilities, we chose to visit the following 3 facilities:

- Gulf Ecology Division, Gulf Breeze, Florida
- Atlantic Ecology Division, Narragansett, Rhode Island
- Ecosystems Research Division, Athens, Georgia

In addition, we used Office of Inspector General audit results from two other ORD site locations. That assessment documented findings related to the IT security of computer rooms at the ORD facility in Las Vegas, Nevada, and the ORD lab in Corvallis, Oregon. The results of these site visits are reported in the OIG Report, *EPA Should Improve Management Practices and Security Controls for Its Network Directory Service System and Related Servers*, Report No. 12-P-0836, September 20, 2012. Appendix A summarizes our findings from all of the assessed ORD facilities.

We used the National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, May 1, 2010, as the template for evaluating IT security controls at ORD labs. We also referred to the U.S. Government Accountability Office *Federal Information System Control Audit Manual*, February 2009, GAO-09-232G, for guidance on general controls categories and for additional descriptions of control activities that should be included in IT security practices.

We designed an assessment tool that covers the following five NIST SP 800-53, Revision 3, security-control families:

- Physical and Environmental Protection
- Access Control
- Media Protection
- System and Communications Protection
- Contingency Planning

We interviewed management at the ORD facilities, ORD program personnel, system administrators, and security personnel. We requested and reviewed the facilities' local procedures, as well as relevant federal and Agency policies and procedures. Further, we conducted tests to verify the implementation and effectiveness of security controls and practices. We did not conduct follow-up audit work because there were no previous reports in this area.

Chapter 2
Agency's Network and Data Vulnerable to Unauthorized Access

ORD facilities do not have established controls that secure or mitigate risks to the Agency's network and data. Specifically, we found that ORD facilities management did not protect wiring closets, Local Area Network access points, and personal computers from unauthorized access. Although we found that ORD management is limiting access to the Agency's network through wireless network access points, the encryption security for these access points can be improved. Agency guidance recommends safeguards that secure networks and data, and mitigate risks from misuse and other security breaches. The weaknesses we identified are the result of facilities management not adhering to and implementing Agency security requirements. Failure to actively manage access to the Agency's network and data can lead to theft, destruction, or the compromise of sensitive information.

Network Connectivity at Risk Due to Unlocked Wiring Closets

By failing to require the use of keys or electronic door locks, ORD facilities management is not restricting access to critical wiring closets. These closets contain cabling and switches that connect facility computers to the LAN and the Agency's network. NIST SP 800-53, Revision 3, recommends securing information system distribution and transmission lines, including the wiring closets. Wiring closets are unsecured because management at the ORD facilities relies on limited security guard patrol to keep buildings and assets protected. Although guard patrols are a compensating control, there are not enough guards to cover the entire site at all times. Unsecured wiring closets increase the likelihood that unauthorized individuals could gain access to the telecommunications areas and damage the networks' wires and cables.

Network at Risk Due to Unrestricted LAN Access and Unpatched PCs

ORD facilities management has not implemented controls over production LAN access to mitigate the risk of a compromised network. When we connected a laptop as an unauthorized device to a random port, we were able to gain access to the network. According to the *Agency Network Security Policy*, the Agency shall implement protective mechanisms that ensure network security by regulating the type and direction of network activities. We were able to make the unauthorized connection because facilities management assumed the port was restricted to the device that was currently connected to the port. An unrestricted port could allow a device that contains viruses or other malware to connect and potentially infect the Agency's network.

We also identified lab PCs connected to the production LAN,[1] which did not have updated security patches. The *Agency Network Security Policy* requires system administrators to apply security patches and upgrades consistent with Agency-approved standards. Management at ORD facilities asserts that applying security patches to these lab computers would cause them to crash and lose research data. Further, lab staff stated that these computers must remain connected to the LAN for printing and research purposes. Without appropriate security patches, viruses and other malware could spread to the production LAN, as well as to other connected components.

Access to Unsecured IT Assets Could Disclose Sensitive Data

ORD management is not protecting IT assets from unauthorized access via internal and external sources. We found workstations with critical financial applications, passwords, and thumb drives left unattended. According to the *Agency Network Security Policy*, EPA personnel, including contractors, are responsible for safeguarding sensitive information, in addition to managing and protecting passwords. However, management does not monitor staff to determine whether they comply with Agency IT security requirements. Failure to safeguard information, follow security guidelines, and monitor compliance could result in sensitive information being modified or stolen.

In addition, our analysis revealed that wireless access point encryption security could be strengthened. The *Agency Network Security Policy* states that information safeguards (such as encryption, data filtering, tagging, or segregation) must be implemented to ensure that sensitive information is protected from disclosure, misuse, or other security breaches. Currently, ORD uses Wired Equivalent Privacy encryption as its wireless security method, which is less secure than Wi-Fi Protected Access or Wi-Fi Protected Access II encryption. However, ORD staff stated that they did not apply more robust security settings to the wireless access points because these access points are not physically or virtually connected to the facilities' network or the LAN. ORD staff further stated that limited security allows easier connection for visitors. Without these security settings, an attacker could launch a "Man-in-the-Middle" attack to intercept the path of communication and masquerade as a legitimate party, such as an EPA facility.

[1] Production LAN is the network in which current systems operate; it is separate from the development or test LAN.

Recommendations

We recommend that the Principal Deputy Assistant Administrator for Research and Development require facilities management personnel at:

1. The Gulf Ecology Division to install locks on all facility wiring closets protecting information technology assets. Additionally, require management personnel at all other ORD facilities to conduct inspections to verify functioning locks on wiring closets protecting information technology assets have been installed.

2. The Gulf Ecology Division to install locks on all facility exterior doors protecting information technology assets. Additionally, require management personnel at all other ORD facilities to verify functioning locks on exterior doors containing information technology assets have been installed.

3. All ORD facilities to configure LAN security software to prevent unauthorized device connection, and isolate or remove unpatched devices from the production LAN.

4. All ORD facilities to perform and document semiannual workstation audits to assess staff compliance with Agency IT security requirements.

5. All ORD facilities to strengthen encryption on all ORD wireless access points.

Agency Response and OIG Evaluation

EPA concurs with the report recommendations. Subsequent to issuance of our draft report, we met with Agency officials to discuss their concerns with the draft report's recommendations. Where appropriate, we modified the report's recommendations to address management's concerns. Appendix B provides the Agency's original response to the draft report. Appendix C provides the crosswalk between the OIG revised recommendations and the Agency's response to those revised recommendations, along with the OIG overall analysis.

Chapter 3
IT Assets Unprotected by Physical and Environmental Controls

Some ORD facilities do not follow established physical and environmental practices that protect IT assets from unauthorized access. These conditions exist, in some cases, due to a failure to enforce existing procedures for securing federal property as documented in local facility security operating procedures. The absence of consistently performed practices compromises the security of significant IT assets and exposes them to theft.

Security Practices for Removal of IT Equipment Are Not Consistently Implemented

Management at some ORD facilities has not consistently implemented local security practices that could prevent the unauthorized removal of IT equipment. For example:

- Security personnel do not inspect vehicles that enter and exit the grounds.
- Front-desk personnel do not, and have not been trained to, examine baggage entering and exiting the facility.
- Security personnel do not examine and compare property passes to employee ID badges to verify authorized removal of IT equipment.

Local standard operating procedures for security guard services and security protection emphasize facility-specific security measures that protect buildings, personnel, and government property. These guard post orders or procedures for security operations stress tasks dedicated to the inspection of vehicles, baggage, briefcases, and property passes. These procedures do exceed federal guidance, but increase the likelihood of detecting unauthorized removal of government property or other suspicious activities. We found that facilities management does not enforce the inspection of employee vehicles, baggage, and property passes because of familiarity with facility employees.

Additionally, we found that while contracted security services personnel are on roving patrol of the facility, there are no security personnel at the facility's main entrance to conduct random inspections and monitor surveillance equipment. Contracted security services personnel are trained in general security services and are further trained in facility-specific security procedures. They are expected to meet minimum qualifications that allow them to conduct surveillance and protect property. Expectations would be that personnel performing the security function in the absence of the contracted security services personnel will be trained and qualified to do so. Without a consistently implemented strategy to prevent the

unauthorized removal of IT equipment or other government property, theft of IT equipment (including sensitive data residing on the equipment) could occur.

Facilities and IT Property Unprotected from Unauthorized Access

ORD IT assets are unguarded and unprotected from unauthorized physical access and removal. First, we noted contractors freely entering and exiting an unlocked room containing production servers that host facility security applications and unsecured electronic key cards that grant access to the facility. Second, we noted ORD staff entering and exiting buildings through unguarded and unmonitored doors, providing no opportunity to monitor baggage that may contain unauthorized items or equipment. Further, during a review of the facility employee separation process, we noted that management has no process for retrieving key cards and vehicle decals from contract employees before they terminate employment at the facility.

NIST SP 800-53, Revision 3, specifies the monitoring of all entry and exit points to account for IT property and authorized access. Further, it specifies that agencies restrict access to *only authorized personnel* in areas where information systems reside.

Unrestricted access to and from these ORD buildings exists because:

- Facilities management is not using locks or key card entry.
- Facilities personnel claim that budget restrictions prevent the monitoring of all building entrances and exits.
- Facilities management has not established a policy requiring contract employees to return key cards and vehicle decals on the final day of their employment.

These weaknesses expose facilities to unauthorized and unrestricted access and do not protect against the removal of valuable IT assets or the destruction of property.

Physical Access to Server Room Unrestricted

Access to the ORD server rooms is not restricted to personnel with direct responsibility for IT equipment. The access control listings show an excessive number of personnel with access to the server rooms. NIST SP 800-53, Revision 3, specifies that organizations authorize physical access to the facility where the information system resides based on position or role. However, LAN administrators are approving access requests without consideration for need or job responsibility. Granting server room access to staff and visitors without a valid purpose poses an increased risk of unauthorized changes to equipment.

Facilities' Closed-Circuit Television System Unequipped to Monitor All Entry Points

ORD facilities have limited camera coverage to monitor all building entrances. In some cases, we found no security cameras at main entrances, lobbies, exit doors, outside the server rooms, or near backup generators. In addition, we observed limited external lighting, which prevents the proper surveillance of areas such as parking lots, building annexes, and storage areas. Lighting should be sufficient to illuminate potential areas of concealment; enhance the observation by guard patrols; and provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility. Site lighting should be coordinated with the closed-circuit television system.

We also found that some facilities had inadequate CCTV digital video storage and playback time. For example, some camera storage and playback time was only 48 to 72 hours; one facility used real-time monitoring, leaving no camera storage and playback time for review.

The Interagency Security Committee's *Physical Security for Federal Facilities* allows the EPA to determine the length of time for which digital images should be stored, based upon facility operations and equipment capabilities. However, ORD facilities have not established the amount of video storage time that is required for retention and inspection purposes. The Security Management Division, Office of Administrative Service, provides guidance that requires the EPA to archive Agency CCTV recordings for up to 1 year at a secure location. Without ample storage and playback time, facilities management will not have enough video to evaluate evolving security incidents.

Recommendations

We recommend that the Principal Deputy Assistant Administrator for Research and Development require facilities management personnel at:

6. The Atlantic Ecology Division and Ecosystems Research Division to guard the facility entrances and exits to facilitate random checks of vehicles, baggage, and property passes. Additionally, require management personnel at all other ORD facilities to adhere to local facility security procedures if random checks of vehicles, baggage, and property passes are required.

7. The Atlantic Ecology Division to train all main-entrance personnel to inspect badges, baggage, and property passes. Additionally, require management personnel at all other ORD facilities to train, if needed, its main-entrance personnel on any required local facility security procedures for inspecting badges, baggage, and property passes at building entrances.

8. All ORD facilities to lock the door to the room containing servers that host facility security applications or move servers to a secure location.

9. All ORD facilities to include contract employees in the facilities' employment separation policy and procedures.

10. All ORD facilities to formalize a process that restricts access to ORD server rooms based upon job responsibility and need.

11. The Gulf Ecology Division and Atlantic Ecology Division to improve camera-monitoring systems and lighting to increase visibility at sites; and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits. Additionally, require management personnel at all other ORD facilities to review camera-monitoring systems and lighting to ensure the equipment is functioning properly to facilitate monitoring of external buildings, server rooms, hallways, storage areas, and entries and exits.

12. The Gulf Ecology Division and Atlantic Ecology Division to increase CCTV monitoring storage time to meet EPA-approved storage requirements. Additionally, require management personnel at all other ORD facilities to review its practices to ensure CCTV monitoring storage time meets EPA-approved storage requirements.

Agency Response and OIG Evaluation

EPA concurs with recommendations 6 through 10. Management does not concur with recommendations to improve CCTV functionality, to improve monitoring of ORD facilities, or to increase CCTV monitoring storage time. Management follows Interagency Security Committee physical security standards, and these standards do not define minimum coverage or minimum recording capacity for CCTV systems. However, *Closed-Circuit Television (CCTV) Systems Guidance* requires the EPA to archive Agency CCTV recordings for up to 1 year at a secure location. As such, it is incumbent upon management to assess the risks and implement appropriate controls. We found the lack of adequate building lighting and CCTV makes the system ineffective for properly monitoring the facilities. Furthermore, CCTV storage capacity is inadequate for aiding management's research if a security breach or incident occurs.

Subsequent to issuance of our draft report, we met with Agency officials to discuss their concerns with the report's recommendations. Where appropriate, we modified the report's recommendations to address management's concerns. Appendix B provides the Agency's original response to the draft report. Appendix C provides the crosswalk between the OIG revised recommendations and the Agency's response to those revised recommendations, along with the OIG overall analysis.

Chapter 4
Facilities Unprepared to Continue Operations in Emergency Situations

ORD facilities have not tested, identified, or executed preventative planning measures to ensure continuous business operations in the event of an emergency or an unauthorized information disclosure. This occurred because ORD facilities did not adhere to minimum security controls recommended by federal guidance. Without these controls in place, ORD facilities could encounter a disruption in business operations and experience a breach of sensitive information.

Sanitized Media Untested for Removal of Sensitive Information

ORD facilities are not testing sanitized media, such as hard drives, to ensure future users do not obtain sensitive information. During our audit, we found that media is sanitized in-house by the degaussing method. Degaussing any current-generation hard disk will render the drive permanently unusable. This means that a magnetized degaussing machine scans a hard drive until the heads of the drive move, which signals the hard drive has been scrambled and is presumed to be no longer functional. However, according to the Agency's Disk Sanitization Procedures, for drives sanitized at the facility, IT personnel must test the drives on a random basis to ensure the removal of all sensitive data. Our review found that facility IT personnel rely on the degaussing method to make drives inoperable and unable to maintain data, and did not test sanitized media. However, sanitized media may contain sensitive data that could compromise the Agency if obtained by unauthorized parties and should be tested.

IT Resources Not Identified for Continuity of Business Operations

Continuity of operations plans for ORD facilities do not identify IT equipment needs and the availability of IT equipment in the event of a COOP emergency. ORD COOP plans did not properly identify IT equipment needed to prepare alternative worksites, known as cold sites. In addition, the ORD COOP plans did not provide listings of local stores from which to purchase IT equipment or the names of government purchase cardholders authorized for procurement for each ORD facility.

NIST SP 800-53, Revision 3, specifies ensuring that equipment and supplies required to resume operations are available at the alternate site, or contracts should be in place to support delivery of equipment and supplies to the site in time to support the agency-defined time period for resumption of business operations. In addition, the publication specifies that the organization establish an alternate processing site, including necessary agreements to permit the resumption

of information system operations for essential mission and business functions when primary processing capabilities are unavailable.

ORD COOP plans do not include these details because ORD management did not provide instructions for documenting IT equipment needs and usage in the event of an emergency. Without defining and documenting IT equipment needs and usage in the COOP plan, ORD labs may experience delays in the resumption of business operations in the event of a COOP emergency.

Critical Backup Media Not Stored Offsite for Continuity of Business Operations

ORD facilities do not have offsite backup data, as federal guidance prescribes. According to NIST SP 800-53, Revision 3, agencies are responsible for ensuring the recovery of data by storing backup copies of the data, the operating system, and other critical information system software in a separate facility or fire-rated container that is not co-located in the same physical area. ORD facilities store backup tapes onsite because they rely on the primary site's fire-rated containers to protect backup copies of data. However, if a geographic disaster destroys the primary site, backup data will be destroyed as well, hindering resumption of business operations.

Tested Emergency Power Supply and Water-Detection Devices Needed for Continuity of Business Operations

We found that server rooms were untested for uninterrupted power supply, which ensures continuous operations in the event of a disaster. According to NIST SP 800-53, Revision 3, agencies are responsible for short-term uninterrupted power supply for the orderly shutdown of information systems in the event of a primary power source loss. In addition, Office of Management and Budget Circular A-130, Appendix III, suggests that agencies have contingency planning activities established and periodically tested in the event of service interruptions. ORD IT personnel stated that they do not conduct testing of the uninterrupted power supply due to the disruption of operations that would occur in the event of a failed test. When asked, ORD IT personnel were not able to provide testing documents or guidance for establishing preventative controls. ORD facilities could face significant delays in restoring power if uninterrupted power supplies do not perform as they should.

Moreover, we found servers placed under charged, wet-piped fire suppression systems.[2] At each facility we visited, we observed sprinklers located directly above server racks, leaving them subject to water damage in the event of leakage.

[2]In wet-piped sprinkler systems, the most common of all sprinkler systems, water remains in the overhead piping until a head fuses, causing the water pressure to force the water out to suppress a fire.

According to OMB Circular A-123, management is responsible for ensuring an effective internal control environment is sustained. ORD management stated that in the event of an emergency, protecting personnel is a higher priority than protecting IT equipment. However, placing the servers under wet-pipe sprinkler systems could lead to water damage, loss of critical scientific data, and loss of backup tapes stored in server rooms.

Similarly, sensors to detect water leakage or flooding are not installed in server rooms at ORD facilities. Our audit results found that ORD management did not plan a strategy to address water-leakage events in the server room. The inability to detect and alert IT personnel about server room flooding increases the likelihood of damage to the server room and IT equipment, and could result in a disruption of business operations.

Recommendations

We recommend that the Principal Deputy Assistant Administrator for Research and Development require facilities management personnel at:

13. All ORD facilities to develop and employ procedures for the random testing of sanitized drives to verify the removal of sensitive information.

14. The Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to update contingency plans to include:

    a. A list of required IT equipment provisions for essential staff in the event of an emergency.
    b. A list of local stores and vendors from which to procure IT equipment in order to maintain operations in an emergency.
    c. Procurement procedures and the names of authorized purchase cardholders in COOP plans for each ORD facility.

    Additionally, require management personnel at all other ORD facilities to provide operational resources and facilities in the event of an emergency.

15. All ORD facilities to relocate data backup tapes offsite to a secure location.

16. All ORD facilities to conduct and document annual tests (during non-business hours) of the uninterrupted power supply connected to servers.

17. The Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to move the server racks so that they are not located directly under sprinkler heads or water pipes, or install leak shields on sprinkler heads located above the server racks to comply with NIST SP 800-53 requirements. If management decides to accept the risk of not

relocating the server racks, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.

18. All ORD facilities to develop a strategy that addresses limiting water damage to IT assets located in the server room and include:

    a. A 24 hours/day, 7 days/week monitoring provision.
    b. Timely actions to be taken in the event of water leaks in the server room.

    If management decides to accept the risk of not developing a strategy to comply with NIST SP 800-53 requirements, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.

Agency Response and OIG Evaluation

EPA concurs with recommendations 13 through 16. Management does not concur with recommendations to improve the server room environmental controls to protect the servers from accidental water damage. Management cites that installing a shield could create an obstruction that could interrupt the water discharge and result in the loss of life. Management also states the fire protection systems are zoned in a manner to only discharge water in the area(s) that require fire suppression, and if a leak occurs, the water and/or air pressure will drop and result in an alarm.

Our audit revealed many of the ORD servers in question sit directly under the sprinkler head, and the risks from accidental water damage could be reduced by rearranging the servers within the room. However, it is incumbent upon management to assess the risks for not implementing these needed measures. Furthermore, when specified in federal guidance, management should document its decisions within the organization's information system security plan. Additionally, we requested documentation governing the fire system design and alarm system. Management had not provided this information. Therefore, we consider these recommendations unresolved.

Subsequent to issuance of our draft report, we met with Agency officials to discuss their concerns with the report's recommendations. Where appropriate, we modified the report's recommendations to address management's concerns. Appendix B provides the Agency's original response to the draft report. Appendix C provides the crosswalk between the OIG revised recommendations and the Agency's response to those revised recommendations, along with the OIG overall analysis.

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	5	Require facilities management personnel at the Gulf Ecology Division to install locks on all facility wiring closets protecting information technology assets. Additionally, require management at all other ORD facilities to conduct inspections to verify functioning locks on wiring closets protecting information technology assets have been installed.	U	Principal Deputy Assistant Administrator for Research and Development			
2	5	Require facilities management personnel at the Gulf Ecology Division to install locks on all facility exterior doors protecting information technology assets. Additionally, require management at all other ORD facilities to verify functioning locks on exterior doors containing information technology assets have been installed.	U	Principal Deputy Assistant Administrator for Research and Development			
3	5	Require facilities management personnel at all ORD facilities to configure LAN security software to prevent unauthorized device connection, and isolate or remove unpatched devices from the production LAN.	U	Principal Deputy Assistant Administrator for Research and Development			
4	5	Require facilities management personnel at all ORD facilities to perform and document semiannual workstation audits to assess staff compliance with Agency IT security requirements.	U	Principal Deputy Assistant Administrator for Research and Development			
5	5	Require facilities management personnel at all ORD facilities to strengthen encryption on all ORD wireless access points.	U	Principal Deputy Assistant Administrator for Research and Development			
6	8	Require facilities management personnel at the Atlantic Ecology Division and Ecosystems Research Division to guard facility entrances and exits to facilitate random checks of vehicles, baggage, and property passes. Additionally, require management at all other ORD facilities to adhere to local facility security procedures if random checks of vehicles, baggage, and property passes are required.	U	Principal Deputy Assistant Administrator for Research and Development			
7	8	Require facilities management personnel at the Atlantic Ecology Division to train all main-entrance personnel to inspect badges, baggage, and property passes. Additionally, require management at all other ORD facilities to train, if needed, its main-entrance personnel on any required local facility security procedures for inspecting badges, baggage, and property passes at building entrances.	U	Principal Deputy Assistant Administrator for Research and Development			

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
8	9	Require facilities management personnel at all ORD facilities to lock the door to the room containing servers that host facility security applications or move servers to a secure location.	U	Principal Deputy Assistant Administrator for Research and Development			
9	9	Require facilities management personnel at all ORD facilities to include contract employees in the facilities' employment separation policy and procedures.	U	Principal Deputy Assistant Administrator for Research and Development			
10	9	Require facilities management personnel at all ORD facilities to formalize a process that restricts access to ORD server rooms based upon job responsibility and need.	U	Principal Deputy Assistant Administrator for Research and Development			
11	9	Require facilities management personnel at the Gulf Ecology Division and Atlantic Ecology Division to improve camera-monitoring systems and lighting to increase visibility at sites; and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits. Additionally, require management at all other ORD facilities to review camera-monitoring systems and lighting to ensure the equipment is functioning properly to facilitate monitoring of external buildings, server rooms, hallways, storage areas, and entries and exits.	U	Principal Deputy Assistant Administrator for Research and Development			
12	9	Require facilities management personnel at the Gulf Ecology Division and Atlantic Ecology Division to increase CCTV monitoring storage time to meet EPA-approved storage requirements. Additionally, require management at all other ORD facilities to review its practices to ensure CCTV monitoring storage time meets EPA-approved storage requirements.	U	Principal Deputy Assistant Administrator for Research and Development			
13	12	Require facilities management personnel at all ORD facilities to develop and employ procedures for the random testing of sanitized drives to verify the removal of sensitive information.	U	Principal Deputy Assistant Administrator for Research and Development			
14	12	Require facilities management personnel at the Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to update its contingency plans to include: a. A list of required IT equipment provisions for essential staff in the event of an emergency. b. A list of local stores and vendors from which to procure IT equipment in order to maintain operations in an emergency. c. Procurement procedures and the names of authorized purchase cardholders in COOP plans for each ORD facility. Additionally, require management personnel at all other ORD facilities to provide operational resources and facilities in the event of an emergency.	U	Principal Deputy Assistant Administrator for Research and Development			
15	12	Require facilities management personnel at all ORD facilities to relocate data backup tapes offsite to a secure location.	U	Principal Deputy Assistant Administrator for Research and Development			

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
16	12	Require facilities management personnel at all ORD facilities to conduct and document annual tests (during non-business hours) of the uninterrupted power supply connected to servers.	U	Principal Deputy Assistant Administrator for Research and Development			
17	12	Require facilities management personnel at the Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to move the server racks so that they are not located directly under sprinkler heads or water pipes, or install leak shields on sprinkler heads located above the server racks to comply with NIST SP 800-53 requirements. If management decides to accept the risk of not relocating the server racks, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.	U	Principal Deputy Assistant Administrator for Research and Development			
18	13	Require facilities management personnel at all ORD facilities to develop a strategy that addresses limiting water damage to IT assets located in the server room and include: a. A 24 hours/day, 7 days/week monitoring provision. b. Timely actions to be taken in the event of water leaks in the server room. If management decides to accept this risk of not developing a strategy to comply with NIST SP 800-53 requirements, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.	U	Principal Deputy Assistant Administrator for Research and Development			

[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

Findings and Recommendations by Site

Table A-1: Findings and recommendations by ORD site

Issue reviewed	Recommendations	GED[a]	ORD Las Vegas	AED[b]	ERD[c]	ORD Corvallis
		X = Weakness found at location				
Network cables and switches exposed to tampering (p. 3)	Install locks on all facility wiring closets.	X				
	Install locks on exterior doors to buildings that contain IT assets.	X				
Port security not configured and PC security patches outdated (pp. 3–4)	Configure LAN security software to prevent unauthorized device connection, and isolate or remove unpatched devices from the production LAN.				X	
ORD workstations left unattended (p. 4)	Perform and document semiannual workstation audits to assess staff compliance with Agency IT security requirements.	X		X	X	
Wireless LAN connection unsecured (p. 4)	Strengthen encryption on all ORD wireless access points.	X				
IT equipment susceptible to unauthorized removal (p. 6)	Guard entrances and exits to facilitate random checks of vehicles, baggage, and property passes.	X		X	X	
	Train all main-entrance personnel to inspect badges, baggage, and property passes.			X		
Key cards and host servers unsecured (p. 7)	Lock the door to the room containing servers that host facility security applications or move servers to a secure location.				X	

Issue reviewed	Recommendations	GED[a]	ORD Las Vegas	AED[b]	ERD[c]	ORD Corvallis
		X = Weakness found at location				
Retrieval of contract employee key cards not consistently performed (p. 7)	Include contract employees in the facilities' employment separation policy and procedures.				X	
Excessive authorized server room access (p. 7)	Formalize a process that restricts access to ORD server rooms based upon job responsibility and need.	X		X	X	X
Facilities not fully monitored by CCTV system building access points (pp. 7–8)	Improve camera-monitoring systems and lighting to increase visibility at sites; and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits.	X	X	X		X
	Increase the CCTV monitoring storage time to meet EPA-approved storage requirements.	X	X	X		X
Untested media drives do not ensure removal of Agency information (p. 10)	Develop and employ procedures for the random testing of sanitized drives to verify the removal of sensitive information.			X	X	
COOP plan outdated (pp. 10–11)	Update ORD COOP plans to include: a. A list of the required IT equipment provisions for essential staff in the event of an emergency.	X		X	X	
	b. A list of local stores and vendors to procure IT equipment from in order to maintain operations in an emergency.	X		X	X	
	c. Procurement procedures and the names of authorized purchase cardholders in COOP plans for each ORD facility.	X		X	X	

Issue reviewed	Recommendations	GED[a]	ORD Las Vegas	AED[b]	ERD[c]	ORD Corvallis
		X = Weakness found at location				
Backup tapes stored onsite (p. 11)	Relocate data backup tapes offsite to a secure location.	X		X	X	
Server rooms untested for uninterrupted power supplies, and network cables and switches exposed to tampering (p. 11)	Conduct and document annual tests (during non-business hours) of the uninterrupted power supply connected to servers.			X	X	
No water sensors installed in server room (p. 12)	Move the server racks so that they are not located directly under sprinkler heads or water pipes, or install leak shields on or above the server racks.	X		X	X	X
	Develop a strategy that addresses limiting water damage to IT assets located in the server room and include: a. A 24 hours/day, 7 days/week monitoring provision. b. Timely actions to be taken in the event of a water leak in the server room.	X				X

Source: OIG analysis of field work results.

[a] Gulf Ecology Division
[b] Atlantic Ecology Division
[c] Ecosystems Research Division

Agency Response to Draft Report

MEMORANDUM

SUBJECT: Office of Research and Development (ORD) Response to the Office of Inspector General (OIG)'s Draft Report entitled, *"Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities,"* dated October 31, 2012

FROM: Lek G. Kadeli, Principal Deputy Assistant Administrator

TO: Arthur Elkins, Inspector General
Office of Inspector General

Thank you for the opportunity to review and comment on OIG's Draft Report, *"Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities."* Our comments are noted below.

The OIG report contained findings and recommendations concerning physical security at ORD facilities as well as information technology security. Office of Administration and Resources Management, Security Management Division (SMD) provides overarching guidance to the Agency regarding physical security issues and was consulted on this response.

We agree with SMD that the OIG review should have applied the Interagency Security Committee (ISC) standards document entitled, "*Physical Security Criteria for Federal Facilities*," dated April 2012, in addition to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations,"* which served as OIG's primary basis for evaluation. NIST 800-53 contain security recommendations for federal information systems, whereas the ISC standards apply to federal facilities. The ISC standards take into account a facility's assigned Facility Security Level (FSL) and have graduated security measures associated with the FSLs.

Moreover, SMD conducts routine vulnerability (security) assessments at EPA facilities. The SMD assessments and recommendations for each EPA facility are tailored to their assigned Facility Security Level, in accordance with the ISC standards. Individual ORD sites have Physical Security Plans that reflect their designated Facility Security Level. Therefore, ORD believes that the OIG's findings and the resulting recommendations should be specific to the sites where vulnerabilities were detected and not generalized to all ORD facilities.

Detailed comments addressing each of the OIG's recommendations are provided in the attachment. If you have any questions regarding this response, please contact Deborah Heckman at (202) 564-7274.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
1	Direct facilities management at all ORD facilities to install locks on all facility wiring closets.	ORD/OARS	ORD concurs. However, note that the deficiency was only found at one facility (GED), and the recommended action is complete. ORD/OARS prefers that the recommendation only be directed to the facility where the finding was noted. ORD facilities have been made aware that this deficiency was noted at one facility, and therefore that all ORD facilities should review their status and take corrective actions if the deficiency exists.
2	Direct facilities management at all ORD facilities to install locks on exterior doors to buildings that contain IT assets.	ORD/OARS	ORD non-concurs. All facilities have exterior door locks.
3	Direct facilities management at all ORD facilities to configure LAN security software to prevent unauthorized device connection, and isolate or remove unpatched devices from the production LAN.	ORD/OSIM	ORD concurs. Initial site specific findings from audit have been corrected. To address this issue at all ORD remote sites, ORD/OSIM will continue implementation of the ORD Baseline Switch project. This effort addresses implementing a standard set of secure configuration settings that prevent unauthorized device connections to the production LAN. ORD/OSIM conducts patching as required by the Agency Computer Security Incident Response Capability (CSIRC). As un-patched systems are identified in various agency reports and operational efforts, these systems will be reviewed and brought up to the necessary patch level.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
4	Direct facilities management at all ORD facilities to perform and document semiannual workstation audits to assess staff compliance with Agency IT security requirements.	ORD/OSIM	ORD concurs. ORD/OSIM will coordinate performance of semiannual workstations audits at all ORD sites to assess staff compliance with Agency IT security requirements. In addition to semiannual audits, ORD/OSIM will create an ORD informational message to educate ORD personnel on securing workstations and portable devices as required by Agency IT Security policy.
5	Direct facilities management at all ORD facilities to strengthen encryption on all ORD wireless access points.	ORD/OSIM	ORD concurs. Corrective actions have been completed. ORD/OSIM has completed a review and confirmed that encryption levels on all ORD Guest WLAN implementations at ORD remote sites meet the ORD standard and OIG recommendation. This action was confirmed completed on 11/26/12. ORD requests closure of this recommendation.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
6	Direct facilities management at all ORD facilities to guard facility entrances and exits to facilitate random checks of vehicles, baggage, and property passes.	ORD/OARS	ORD non-concurs. Security Management Division (SMD) conducts routine vulnerability (security) assessments at EPA facilities. Assessments and recommendations are driven by the assigned Facility Security Level in accordance with Interagency Security Committee standards. Individual ORD sites have Physical Security Plans that reflect their designated Facility Security Level and measures tailored to their location and vulnerability assessment. The single recommendation proposed is not appropriate for all sites. Physical security assessments and recommendations should align with SMD reports and reflect their designated security level. Minimum recommendations are summarized in the EPA Minimum Security Requirements found at http://intranet.epa.gov/oa/smd/pdfs/ps-dat-security-requirements_final_0507.pdf .

Rec No.	OIG Recommendation	Responsible Office	ORD Response
7	Direct facilities management at all ORD facilities to train all main-entrance personnel to inspect badges, baggage, and property passes.	ORD/OARS	ORD non-concurs. Security Management Division (SMD) conducts routine vulnerability (security) assessments at EPA facilities. Assessments and recommendations are driven by the assigned Facility Security Level in accordance with Interagency Security Committee standards. Individual ORD sites have Physical Security Plans that reflect their designated Facility Security Level and measures tailored to their location and vulnerability assessment. The single recommendation proposed is not appropriate for all sites. Physical security assessments and recommendations should align with SMD reports and reflect their designated security level. Minimum recommendations are summarized in the Environmental Protection Agency Minimum Security Requirements found at http://intranet.epa.gov/oa/smd/pdfs/ps-dat-security-requirements_final_0507.pdf .
8	Direct facilities management at all ORD facilities to lock the door to the room containing servers that host facility security applications or move servers to a secure location.	ORD/OARS	ORD concurs. All servers in ORD/ERD are now secured behind locked doors.
9	Direct facilities management at all ORD facilities to include contract employees in the facilities' employment separation policy and procedures.	ORD/OARS	ORD concurs. ORD/ERD now has a procedure for processing separated contract employees. The procedure includes collecting keys, badges, swipe cards and parking permits.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
10	Direct facilities management at all ORD facilities to formalize a process that restricts access to ORD server rooms based upon job responsibility and need.	ORD/OSIM	ORD concurs. ORD/OSIM and facilities staff reviewed and remediated specific findings from the audit to ensure that server room access lists ensure only personnel with job duties requiring unescorted access to server rooms are permitted entry. ORD/OSIM will create formal procedures for the review and management of server room access will be created.
11	Direct facilities management at all ORD facilities to improve camera-monitoring systems and lighting to increase visibility at sites; and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits.	ORD/OARS	ORD non-concurs. Security Management Division (SMD) conducts routine vulnerability (security) assessments at EPA facilities. Assessments and recommendations are driven by the assigned Facility Security Level in accordance with Interagency Security Committee standards. Individual ORD sites have Physical Security Plans that reflect their designated Facility Security Level and measures tailored to their location and vulnerability assessment. The single recommendation proposed is not appropriate for all sites. Physical security assessments and recommendations should align with SMD reports and reflect their designated security level. Minimum recommendations are summarized in the Environmental Protection Agency Minimum Security Requirements found at http://intranet.epa.gov/oa/smd/pdfs/ps-dat-security-requirements_final_0507.pdf. It should be noted that although not required, ORD has taken proactive steps beyond the EPA Minimum Security Requirements by increasing CCTV data storage capability at several locations.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
12	Direct facilities management at all ORD facilities to increase the CCTV monitoring storage time to meet EPA-approved storage requirements.	ORD/OARS	ORD non-concurs. Security Management Division (SMD) conducts routine vulnerability (security) assessments at EPA facilities. Assessments and recommendations are driven by the assigned Facility Security Level in accordance with Interagency Security Committee standards. Individual ORD sites have Physical Security Plans that reflect their designated Facility Security Level and measures tailored to their location and vulnerability assessment. The single recommendation proposed is not appropriate for all sites. Physical security assessments and recommendations should align with SMD reports and reflect their designated security level. Minimum recommendations are summarized in the Environmental Protection Agency Minimum Security Requirements found at http://intranet.epa.gov/oa/smd/pdfs/ps-dat-security-requirements_final_0507.pdf. It should be noted that although not required, ORD has taken proactive steps beyond the EPA Minimum Security Requirements by increasing CCTV data storage capability at several locations.
13	Direct facilities management at all ORD facilities to develop and employ procedures for the random testing of sanitized drives to verify the removal of sensitive information.	ORD/OSIM	ORD concurs. The ORD Electronic Media Sanitization Standard Operating Procedure (SOP) was updated on August 6, 2012. This SOP update identified the requirement for validating the success of sanitization efforts. ORD/OSIM will communicate this requirement by distributing this procedure to staff who perform this duty.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
14	Direct facilities management at all ORD facilities to update ORD COOP plans to include: a. A list of required IT equipment provisions for essential staff in the event of an emergency. b. A list of local stores and vendors to procure IT equipment from in order to maintain operations in an emergency. c. Procurement procedures and the names of authorized purchase cardholders in COOP plans for each ORD facility.	ORD/OARM	ORD non-concurs. EPA Order 2030.1A, *Continuity of Operations (COOP) Policy* is the Agency's contingency planning policy for identification of COOP site requirements. ORD laboratories (except for those physically located in RTP and Cincinnati, where OARM has the COOP lead) were excluded from the Order as they do not directly support Agency mission essential functions (MEFs). Under NIST 800-34 Rev 1 (page 18), "Information systems that do not support COOP functions do not require alternate sites as part of the ISCP (Information System Contingency Plan) recovery strategy..." Therefore, ORD laboratories are not required to maintain alternate work sites.
15	Direct facilities management at all ORD facilities to relocate data backup tapes offsite to a secure location.	ORD/OSIM	ORD concurs. ORD/OSIM is configuring ORD sites to backup data over the Agency WAN to geographically dispersed primary and secondary backup locations. Many ORD remote sites have transitioned into this configuration, while others are planning to do so as budget and resources permit. ORD/OSIM will review ORD remote site data that is not currently included in this plan to determine the need for back-up based on the criticality of the data. Additionally, ORD/OSIM will determine operational and cost implications of completing an electronic backup or secure remote storage of back-up tapes for this data.

Rec No.	OIG Recommendation	Responsible Office	ORD Response
16	Direct facilities management at all ORD facilities to conduct and document annual tests (during non business hours) of the uninterrupted power supply connected to servers.	ORD/OSIM	ORD concurs. ORD/OSIM will conduct further research to determine the operational feasibility and cost implications of conducting and documenting annual UPS testing for ORD servers.
17	Direct facilities management at all ORD facilities to move the server racks so that they are not located directly under sprinkler heads or water pipes, or install leak shields on or above the server racks.	ORD/OARS	ORD non-concurs. ORD server rooms are in compliance with the National Fire Protection Association (NFPA) standards. NFPA A.5.2.1.2 requires 18 inches of clearance below the sprinkler deflector. Installing a shield could create an obstruction that would interrupt the water discharge and result in the loss of life.
18	Direct facilities management at all ORD facilities to develop a strategy that addresses limiting water damage to IT assets located in the server room and include: a. A 24 hours/day, 7 days/week monitoring provision. b. Timely actions to be taken in the event of water leaks in the server room.	ORD/OARS	ORD non-concurs. Server rooms are in compliance with the National Fire Protections Association (NFPA) standards. Fire protection systems are zoned in a manner to only discharge water in the area(s) that require fire suppression. In addition, if a leak occurs, the water and/or air pressure will drop and result in an alarm.

Appendix C

Agency Response to OIG Revised Recommendations

Subsequent to the issuance of our draft report, we met with Agency officials to discuss their concerns with the report's recommendations. Where appropriate, we modified the report's recommendations to address management's concerns and provided the agency with a copy of the revised recommendations for comment. Management concurred with four of the revised recommendations, but provided suggested changes to the wording in seven of our revised recommendations. OIG made no additional modifications based on ORD's suggested wording of our revised recommendations.

Management does not concur with the recommendations to improve the server room environmental controls to protect the servers from accidental water damage (recommendations 17 and 18, respectively). Management states that installing a shield could create an obstruction that could interrupt the water discharge and result in the loss of life. Management also states the fire protection systems are zoned in a manner to only discharge water in the area(s) that require fire suppression, and if a leak occurs, the water and/or air pressure will drop and result in an alarm. Our audit revealed many of the ORD servers in question sit directly under the sprinkler head, and the risks from accidental water damage could be reduced by rearranging the servers within the room. However, it is incumbent upon management to assess the risks to assets and document decisions within the organization's information system security plan as required by federal guidance. Therefore, the OIG made no additional modifications based on the suggested wording of our revised recommendations.

This appendix represents the crosswalk between the OIG revised recommendations and the ORD response to those revised recommendations, along with suggested wording to our revised recommendations.

Rec No.	OIG Revised Recommendation	New ORD Response	ORD Suggested Alternative/Revised Recommendation	OIG Overall Analysis
2	Require facilities management personnel at the Gulf Ecology Division to install locks on all facility exterior doors protecting information technology assets. Additionally, require management at all other ORD facilities to verify functioning locks on exterior doors containing information technology assets have been installed.	Concur- however, ORD suggests minor changes to the wording. In addition, ORD has already implemented this recommendation and we recommend that this be closed as completed.	Direct facilities management at the Gulf Ecology Division to install locks on all facility exterior doors protecting information technology assets. Additionally, direct ORD facilities management to ensure that local security procedures and policies for locks on exterior doors protecting information technology assets are being followed.	Although ORD concurred with our revised recommendation, no documented evidence was provided to indicate ORD implemented the recommendation at all ORD locations. Therefore, this recommendation will remain open. Furthermore, the OIG made no additional modifications based on the ORD suggested wording of our revised recommendation.
6	Require facilities management personnel at the Atlantic Ecology Division and Ecosystems Research Division to guard facility entrances and exits to facilitate random checks of vehicles, baggage, and property passes. Additionally, require management at all other ORD facilities to adhere to local facility security procedures if random checks of vehicles, baggage, and property passes are required.	Concur- however, ORD suggests changes to the wording. Also, ORD follows Interagency Security Committee physical security standards, as applied to our facilities in collaboration with the Security Management Division. Further, ORD facilities adhere to local security procedures and policies appropriate to the local security environment. The Ecosystems Research Division revised the security policy to eliminate the conflict between policy and accepted procedure.	Direct facilities management at the Atlantic Ecology Division and Ecology Research Division to guard facility entrances and exits to facilitate random checks of vehicles, baggage, and property passes. Direct facilities management at ORD facilities to ensure that local security procedures and policies for the guarding of facility entrances and exits and random checking of vehicles, baggage, and property passes, where applicable, are being followed.	Although ORD concurred with our revised recommendation and provided the OIG with suggested wording for the recommendation, the OIG made no additional modifications to the revised recommendation since our recommendation to management is more direct and action-oriented.
7	Require facilities management personnel at the Atlantic Ecology Division to train all main-entrance personnel to inspect badges, baggage, and property passes. Additionally, require management at all other ORD facilities to train, if needed, its main-entrance personnel on any required local facility security procedures for inspecting badges, baggage, and property passes at building entrances.	Concur- however, ORD suggests changes to the wording. In addition, please note that ORD follows Interagency Security Committee physical security standards, as applied to our facilities in collaboration with the Security Management Division. Further, ORD facilities adhere to local security procedures and policies appropriate to the local security environment.	Direct facilities management at the Atlantic Ecology Division to train all main-entrance personnel to inspect badges, baggage, and property passes. Direct facilities management at ORD facilities to ensure that local security procedures and policies for the guarding of facility entrances and exits and random checking of vehicles, baggage, and property passes, where applicable, are being followed.	Although ORD concurred with our revised recommendation and provided the OIG with suggested wording for the recommendation, the OIG made no additional modifications. We stand by our recommendation, since we found no security personnel at the facility's main entrance to conduct random inspections and monitor surveillance equipment while contracted security services personnel were on patrol of the facility. The expectation would be that personnel performing the security function in the absence of the contracted security services personnel be trained and qualified to do so.

Rec No.	OIG Revised Recommendation	New ORD Response	ORD Suggested Alternative/Revised Recommendation	OIG Overall Analysis
11	Require facilities management personnel at the Gulf Ecology Division and Atlantic Ecology Division to improve camera-monitoring systems and lighting to increase visibility at sites; and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits. Additionally, require management at all other ORD facilities to review camera-monitoring systems and lighting to ensure the equipment is functioning properly to facilitate monitoring of external buildings, server rooms, hallways, storage areas, and entries and exits.	Non-Concur. ORD follows Interagency Security Committee physical security standards. Current standards suggest CCTV systems for facilities designated security levels 1, 2, and 3. Interagency Security Committee does not define minimum coverage or minimum recording capacity for CCTV systems. Please note: Gulf Ecology Division, a Level 2 facility, upgraded their existing CCTV system as did Atlantic Ecology Division, a Level 3 facility.	Per 2750, ORD's alternative recommendation is: Direct facilities management at the Gulf Ecology Division and Atlantic Ecology Division to improve camera-monitoring systems and lighting to increase visibility at sites and to monitor external buildings, server rooms, hallways, storage areas, and entries and exits. Additionally, direct facilities management at ORD to ensure that local security procedures and policies to improve the effectiveness of camera-monitoring systems and lighting and the monitoring of external buildings, server rooms, hallways, storage areas, and entries and exits, where applicable, are being followed.	Management does not concur with this recommendation to improve CCTV functionality or to improve monitoring of ORD facilities. Management stated they follow Interagency Security Committee physical security standards and these standards do not define minimum coverage for CCTV systems. However, we found the lack of adequate building lighting and CCTV coverage makes the system ineffective for properly monitoring the facilities. Therefore, the OIG made no additional modifications based on the suggested wording of our revised recommendations
12	Require facilities management personnel at the Gulf Ecology Division and Atlantic Ecology Division to increase the CCTV monitoring storage time to meet EPA-approved storage requirements. Additionally, require management at all other ORD facilities to review its practices to ensure CCTV monitoring storage time meets EPA-approved storage requirements.	Non-concur. ORD follows Interagency Security Committee physical security standards. Current standards suggest CCTV systems for facilities designated security levels 1, 2, and 3. Interagency Security Committee does not define minimum coverage or minimum recording capacity for CCTV systems. Please note: Gulf Ecology Division, a Level 2 facility, upgraded their existing CCTV system as did Atlantic Ecology Division, a Level 3 facility.	Per 2750, ORD's alternative recommendation is: Direct facilities management at the Gulf Ecology Division and Atlantic Ecology Division to increase the CCTV monitoring storage time to meet EPA-approved storage requirements. Direct facilities management at ORD facilities to ensure that CCTV monitoring storage time is increased to meet EPA-approved storage requirements, where applicable.	Management does not concur with this recommendation to increase CCTV monitoring storage time. Management stated they follow Interagency Security Committee physical security standards and these standards do not define minimum recording capacity for CCTV systems. However, we found the CCTV storage capacity inadequate for aiding management's research if a security breach or incident occurs. Therefore, the OIG made no additional modifications based on the suggested wording of our revised recommendations.

Rec No.	OIG Revised Recommendation	New ORD Response	ORD Suggested Alternative/Revised Recommendation	OIG Overall Analysis
14	Require facilities management personnel at the Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to update its contingency plans to include: a. A list of required IT equipment provisions for essential staff in the event of an emergency. b. A list of local stores and vendors from which to procure IT equipment in order to maintain operations in an emergency. c. Procurement procedures and the names of authorized purchase cardholders in COOP plans for each ORD facility. Additionally, require management personnel at all other ORD facilities to provide operational resources and facilities in the event of an emergency.	Concur- however, ORD suggests changes to the wording.	Direct facilities management at the Atlantic Ecology Division to train all main-entrance personnel to inspect badges, baggage, and property passes. Additionally, direct management at all other ORD facilities train, if needed, its main-entrance personnel on any required local facility security procedures for inspecting badges, baggage, and property passes at building entrances. Direct facilities management at the Gulf Ecology Division, Atlantic Ecology Division, and the Ecosystems Research Division to update its contingency plans to include: a. A list of required IT equipment provisions for essential staff in the event of an emergency. b. A list of local stores and vendors to procure IT equipment from in order to maintain operations in an emergency. c. Procurement procedures and the names of authorized purchase cardholders in contingency plans. Additionally, direct management to review and update, if necessary, its contingency plans to ensure resources are available and facilities remain operational, in the event of an emergency.	Although ORD concurred with our revised recommendation and provided the OIG with suggested wording for the recommendation, the OIG made no additional modifications to the revised recommendation since our recommendation to management is more direct and action-oriented.

Rec No.	OIG Revised Recommendation	New ORD Response	ORD Suggested Alternative/Revised Recommendation	OIG Overall Analysis
17	Require facilities management personnel at the Gulf Ecology Division, Atlantic Ecology Division, and Ecosystems Research Division to move the server racks so that they are not located directly under sprinkler heads or water pipes, or install leak shields above the server racks to comply with NIST SP 800-53 requirements. If management decides to accept the risk of not relocating the server racks, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.	Non-Concur. ORD meets National Fire Protections Association A.5.2.1.2 requirements for sprinkler installation. Installing a shield could create an obstruction that could interrupt the water discharge and result in the loss of life.		Moving the server racks or installing leak shields above them would have no effect on obstructing water discharge or result in the loss of life. The purpose of the leak shields is to reduce/prevent accidental water damage to the servers. Based on federal guidance, if management does not want to install the shields or move the servers, then it should update the security plan and have the authorizing official formally accept operating the server room with this know risk.
18	Require facilities management personnel at all ORD facilities to develop a strategy that addresses limiting water damage to IT assets located in the server room and include: a. A 24 hours/day, 7 days/week monitoring provision. b. Timely actions to be taken in the event of water leaks in the server room. If management decides to accept this risk of not developing a strategy to comply with NIST SP 800-53 requirements, then ORD should update the respective information system security plan and have the authorizing official formally accept the responsibility for operating the room with known risks as required by federal policy.	Non-Concur. Server rooms are in compliance with the National Fire Protections Association standards. Fire protection systems are zoned in a manner to only discharge water in the area(s) that require fire suppression. In addition, if a leak occurs, the water and/or air pressure will drop and result in an alarm.		The OIG requested documentation governing the fire system design and alarm system, and ORD has not provided this information. Therefore, this recommendation will remain open.

Appendix D

Distribution

Office of the Administrator
Principal Deputy Assistant Administrator for Research and Development
Associate Assistant Administrator for Research and Development
Deputy Assistant Administrator for Management, Office of Research and Development
Deputy Assistant Administrator for Science, Office of Research and Development
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Senior Agency Information Security Officer
Audit Follow-Up Coordinator, Office of Research and Development