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

JUN 25 2013

MEMORANDUM

OFFICE OF
RESEARCH AND DEVELOPMENT

SUBJECT: Response to the Office of Inspector General (OIG) Final Report No. 13-P-0252 *Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities*, dated May 8, 2013

FROM: for Lek G. Kadeli, Principal Deputy Assistant Administrator
Office of Research and Development (ORD)

TO: Arthur A. Elkins, Jr., Inspector General
Office of the Inspector General (OIG)

Thank you for the opportunity to respond to the OIG Final Report titled, *Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities*. ORD's corrective actions responding to the OIG's recommendations are provided below.

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
1.	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.	All ORD Division Directors in charge of remote facilities will be instructed to conduct inspections to verify functioning locks on information technology closets and make adjustments as necessary.	ORD/OARS	7/31/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
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.	All ORD Division Directors in charge of remote facilities will be instructed to conduct inspections to verify functioning locks on all exterior doors containing information technology assets and make adjustments as necessary.	ORD/OARS	7/31/2013
3.	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.	Implementation of standard configuration settings continue to be applied across ORD LAN switches. Lists of non-compliant configurations are being generated and reviewed. Resource and cost implications are being reviewed as they relate to the completion of these efforts. Cost vs. risk information will be presented to the ORD SIO for decision.	ORD/OSIM	10/1/2013
4.	Require facilities management personnel at all ORD facilities to perform and document semiannual workstation audits to assess staff compliance with Agency IT security requirements.	A draft informational message to educate users on securing workstations and portable devices is currently under development. ORD/OSIM will help coordinate semi-annual workstation audits at all ORD facilities to assess staff compliance with Agency IT security requirements.	ORD/OSIM	11/1/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
5.	Require facilities management personnel at all ORD facilities to strengthen encryption on all ORD wireless access points.	Complete. No further action. Appropriate documentation of completion will be provided to ORD's Audit Liaison.	ORD/OSIM	11/26/2012
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.	All ORD Division Directors in charge of remote facilities will review Physical Security Policies to ensure they reflect Agency-determined security countermeasures for the facility. Adjustments to operating procedures will be made as necessary.	ORD/OARS	9/30/2013
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.	All ORD Division Directors in charge of remote facilities will be instructed to conduct training, as required, to educate staff on security countermeasure requirements identified in the Physical Security Policies.	ORD/OARS	9/30/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
8.	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.	All ORD Division Directors in charge of remote facilities will be instructed to ensure that doors will be locked to rooms containing servers that host facility security applications.	ORD/OARS	9/30/2013
9.	Require facilities management personnel at all ORD facilities to include contract employees in the facilities' employment separation policy and procedures.	All ORD Division Directors in charge of remote facilities will be instructed to include contract employees in the facilities' separation procedures.	ORD/OARS	9/30/2013
10.	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.	ORD/OSIM site maintained documentation will be reviewed to determine and identify which sites and which groups are named as responsible for maintaining access to server rooms. These documents will be updated with additional details as needed of responsibility where it is not currently present. Additional procedures and processes will be written where none exist.	ORD/OSIM	12/15/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
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.	All ORD Division Directors in charge of remote facilities will be instructed to review camera-monitoring systems and lighting to ensure that that equipment is functioning properly.	ORD/OARS	9/30/2013
12.	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.	All ORD Division Directors in charge of remote facilities will be instructed to review CCTV recording capacities to ensure adequacy to meet requirement described in the Physical Security Plan.	ORD/OARS	9/30/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
13.	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.	Although the ORD Electronic Media Sanitization SOP identifies this requirement, additional updates to this SOP are being considered and ORD/OSIM communication is under consideration.	ORD/OSIM	9/15/2013
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.	As EPA Order 2030.1A does not require COOP plans for ORD remote locations, all laboratory continuity documents will be renamed as "Business Continuity Plans" (BCPs) per discussion with the OIG. This is further supported under NIST 800-34 Rev 1 (page 18), where "Information system that do not support COOP functions do not require alternate sites as part of the ISCP (information System Contingency Plan) recovery strategy..." ORD/OPARM will work to ensure that all ORD facilities are reviewing necessary operating plans to adequately prepare for emergency situations, as it relates to overall IT equipment issues.	ORD/OPARM	12/31/2014

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
15.	Require facilities management personnel at all ORD facilities to relocate data backup tapes offsite to a secure location.	ORD/OSIM will coordinate with each site to determine data and/or applications that support critical functions and/or Agency defined Mission Essential Function (MEFs). This data will be considered for inclusion in the current electronic backup effort that is occurring at ORD primary and secondary automated failover processing sites.	ORD/OSIM	12/15/2013
16.	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.	ORD/OSIM site maintained documentation will be reviewed to identify current occurrences of UPS testing as related to ORD managed servers. Documents will be updated with additional details of UPS testing where it is not currently present.	ORD/OSIM	9/15/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
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 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.	All ORD Division Directors in charge of remote facilities will be instructed to review the location of server racks and determine if it is cost beneficial to relocate the racks away from sprinkler heads and water pipes. If relocation is determined to not be cost beneficial, the Division Directors will be instructed to update the system security plan with the cost/benefit information and accept the risk of possible damage and associated replacement costs.	ORD/OARS	12/31/2013

No.	Recommendation	High-Level Intended Corrective Action(s)	Responsible Office	Estimated Completion Date
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.	All ORD Division Directors in charge of remote facilities will be instructed to take action to verify 24/7 moisture detection capacities, installing detection devices in server rooms. If it is determined that installing these moisture detection devices is not cost beneficial, the Division Directors will be instructed to update the system security plan with the cost/benefit information and accept the risk of possible damage and associated replacement costs.	ORD/OARS	12/31/2013

If you have any questions regarding this response, please contact Deborah Heckman at (202) 564-7244.

cc: Ramona Trovato
Bob Kavlock
Alice Sabatini
Jerry Blancato
Amy Battaglia