U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

CSB Needs Better Security Controls to Protect Critical Data Stored on Its Regional Servers

Report No. 16-P-0035 November 5, 2015

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Nancy Dao
Iantha J. Maness

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
FISMA	Federal Information Security Modernization Act of 2014
GSA	U.S. General Services Administration
GSS	General Support System
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
RMF	Risk Management Framework
SP	Special Publication
SSP	System Security Plan
WRO	Western Regional Office of Investigations

Cover photo: CSB Western Regional Office of Investigations in Denver, Colorado. (OIG photo)

Are you aware of fraud, waste or abuse in an EPA or CSB program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

16-P-0035
November 5, 2015

At a Glance

Why We Did This Review

We sought to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of physical and environmental controls at its Western Regional Office of Investigations (WRO), and actions taken to correct prior year information security control weaknesses. The WRO is in Denver, Colorado. Implementing physical and environmental protection controls are important because they are the common controls needed to protect all information technology (IT) assets. These controls serve as the foundation for granting access to the server room and protecting the IT assets and data from harm due to unauthorized access, ineffective fire suppression and humidity control management.

This report addresses the following CSB goal:

- *Preserve the public trust by maintaining and improving organizational excellence.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

CSB Needs Better Security Controls to Protect Critical Data Stored on Its Regional Servers

What We Found

CSB should strengthen physical and environmental protection controls for the WRO server room. CSB also should take steps to implement the remaining four recommendations from the prior year report to resolve security deficiencies cited.

Ineffective physical and environmental protection controls place CSB's investigative data at risk of theft, loss or damage.

Weak physical and environmental controls existed because CSB had not established and disseminated policy and procedures to WRO personnel to inform them of management's requirements for protecting the server room. CSB also had not taken steps associated with the WRO server room to establish access control rosters and physical access logs to control and monitor access. Further, CSB had not (1) implemented procedures to escort visitors, (2) secured the server room keys, (3) installed automatic fire suppression capability, and (4) monitored humidity levels.

As a result of the weaknesses noted, critical CSB network equipment and investigative data may be susceptible to theft, loss or damage.

Recommendations and Planned Agency Corrective Actions

We recommend that CSB establish and disseminate written physical and environmental protection policy and procedures, develop an authorized access roster and physical access log, periodically review and update the roster and the logs to restrict access to the server room, develop escort procedures for server room visitors, secure the server room keys and limit key access to authorized users, and equip the server room with automatic fire suppression capability to protect investigative data critical to CSB's mission.

CSB concurred with our audit recommendations and provided planned corrective actions and completion dates. Based on the CSB's response, OIG considered Recommendation 5 closed and revised Recommendation 7. We agreed with the CSB's plan of corrective actions and estimated completion dates, and consider Recommendations 1, 2, 3, 4, 6 and 7 open with corrective actions pending.

Noteworthy Achievements

In response to prior OIG audit recommendations and this year's audit, CSB took the following actions at its headquarters and WRO server rooms: (1) implemented processes to monitor temperature levels, (2) revised the server room visitor access logs, and (3) installed software to enable automatic orderly shutdown of servers in the event of a power outage.

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

THE INSPECTOR GENERAL

November 5, 2015

The Honorable Vanessa Allen Sutherland
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Ms. Sutherland:

This is our report on the audit of the U.S. Chemical Safety and Hazard Investigation Board's compliance with the Federal Information Security Modernization Act of 2014 for fiscal year 2015 conducted by the Office of Inspector General (OIG). This report contains findings that describe the issues the OIG has identified and corrective actions the OIG recommends.

You are not required to provide a written response to this final report because you agreed with our recommendations and provided planned corrective actions that meet the intent of the recommendations, as well as planned completion dates for each recommendation.

We will post this report to our website at www.epa.gov/oig.

Sincerely,

Arthur A. Elkins

Arthur A. Elkins Jr.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

The Office of Inspector General (OIG) conducted this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2015. In particular, we evaluated CSB's:

- Implementation of physical and environmental protection controls at its Western Regional Office of Investigations (WRO).
- Actions taken to correct prior year information security control weaknesses.

Background

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, dated April 2013, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, lists security controls necessary for organizations to strengthen their information systems and the environments in which those systems operate. NIST SP 800-53 requires, in part, organizations to implement physical and environmental protection controls in the following areas:

- Physical and Environmental Protection Policy and Procedures
- Physical Access Authorizations
- Physical Access Control
- Monitoring Physical Access
- Visitor Access Records
- Emergency Shutoff
- Emergency Power
- Emergency Lighting
- Fire Protection
- Temperature and Humidity Controls
- Water Damage Protection

The CSB's principal role is to investigate chemical accidents to determine the conditions and circumstances that led up to the event and identify the cause or causes so that similar events might be prevented. The CSB is headquartered in Washington, D.C., and has its WRO in a federal center complex in Denver, Colorado. CSB's professional staff includes investigators, engineers, safety experts, attorneys and administrators.

To assist the WRO in carrying out its investigative function, CSB has a server room to maintain data critical to WRO investigations. The U.S. General Services Administration (GSA) is responsible for the management of the complex, which includes providing tenant organizations with the physical space and utilities necessary for the organization to carry out its mission. CSB is responsible for defining its physical and utility needs and implementing the mandated physical and environmental protection controls. Implementing these controls are important to protect servers maintaining data collected during investigations of chemical incidents and hazard and safety studies, CSB's analyses of the data, and the associated investigation results.

Responsible Offices

The CSB's Board Chairperson is responsible for agency administration. Within CSB's Office of Administration are CSB personnel responsible for CSB's information technology (IT) security program. The Chief Information Officer and Deputy Chief Information Officer are responsible for making risk management decisions regarding deficiencies; their potential impact on controls; and the confidentiality, integrity and availability of systems. The Chief Information Officer is also responsible for reporting to the agency head on progress of remedial actions on the agency information security program.

Scope and Methodology

We conducted this audit from May to October 2015 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 conclusions based on our audit objectives.

We reviewed CSB's General Support System's System Security Plan, and CSB's recently drafted policies and procedures related to implementation and management of physical and environmental protection controls for the WRO server room. We reviewed relevant federal criteria and guidance in NIST SP 800-53, Revision 4, for information security control requirements. We also conducted a site visit to the WRO server room to test compliance with federal criteria and NIST guidance for the above controls. We interviewed personnel from CSB headquarters and WRO responsible for developing, implementing and overseeing physical and environmental protection controls. Since the WRO server room is located on a federal center complex, we interviewed a representative from GSA who was responsible for building management of the facility that houses the CSB WRO server room.

CSB completed many of the prior year's audit recommendations. Chapter 3 contains the status of the remaining open prior year's audit recommendations.

Noteworthy Achievements

CSB recently installed an air conditioning unit, an exhaust fan, and door ventilation louvers in the WRO server room to correct an overheating problem and allow proper ventilation. CSB also implemented processes to monitor temperature levels in the CSB headquarters server room and installed software to enable automatic orderly shutdown of CSB headquarters servers in the event of a power outage.

Chapter 2
CSB WRO Server Room Lacks Key Physical and Environmental Protection Controls

CSB's WRO server room lacks key physical and environmental protection controls necessary to protect critical data needed to carry out the WRO's investigative function. NIST requires organizations to implement controls to manage physical access, fire suppression and humidity for server rooms. However, CSB had not established and disseminated policy and procedures to WRO personnel. Specifically, we found that CSB had not implemented required key physical controls involving visitor access to the server room, access control logs, and securing keys. Similarly, CSB had not implemented key environmental controls involving fire suppression capability and monitoring humidity levels. As a result, critical CSB WRO network equipment and investigative data stored on the servers may be susceptible to theft, loss or damage due to unauthorized access or unexpected environmental disruptions.

Key Physical Controls Not in Place

CSB's WRO server room lacked several key physical controls necessary to ensure management knows when someone accesses the room and only authorized personnel or escorted visitors (personnel not on the authorized access list) have access.

NIST SP 800-53, Revision 4, requires, in part, federal organizations to have physical access control; develop and approve the authorized server room access roster or list, and periodically review user access authorizations and update the list; develop, maintain and periodically review the server room physical access log; and maintain and periodically review visitor access records/logs that include such details as the visitor's name, organization, signature, form of identification, dates of access, entry and departure times, purpose of visit, and name and organization of the person escorting the visitor.

The lack of these key controls occurred because CSB did not have written physical protection policy and procedures approved by management. CSB recently drafted, but had not disseminated, its draft policy and procedures for the headquarters and WRO server rooms. Our review of the draft policy and procedures found that they did not include purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance. In addition, the draft policy and procedures did not include detailed procedures to facilitate the implementation of the associated physical and environmental protection controls. CSB had not implemented procedures for maintaining an authorized access roster, developing physical access logs and updating visitor logs, escorting visitors, and securing server room keys. Details follow.

Authorized Access Rosters: CSB did not establish or maintain an access roster of authorized individuals with management's written approval to physically access the WRO server room. The Chief Information Officer indicated that whenever there was a WRO system issue, the Chief Information Officer would call from CSB headquarters and ask an available WRO staff member to go into the server room and verbally detail step-by-step how to fix the issue. Although WRO designated two personnel as key holders for the server room, it did not issue and secure the server room keys based on the designation or appoint specific individuals for authorized access (including job title and duties requiring physical access to server room). NIST requires federal organizations to define and approve the authorized access list. Also, NIST requires periodic review of the authorized access list and the removal of individuals from the authorized access list when access is no longer required.

Physical Access Logs: There was no physical access log developed and used by CSB WRO to monitor and track physical access activities to the server room. Such a log is useful in detecting and investigating physical security incidents to the server room. NIST requires the use, maintenance and periodic review of a physical access log to monitor physical access to the server room for suspicious physical access activities. Due to the absence of the physical access log, CSB will have a more difficult time investigating physical security incidents. To assist in automatically generating a physical access log for entering and exiting the server room, CSB plans to install HSPD-12 PIV Card Access on the server room door.

Visitor Logs: We also found the visitor log used by CSB was not adequate to document important details about the visit for personnel not on the server room authorized access list. The visitor log recorded the visitor's name and agency, date, and time in and time out for those who accessed the server room since June 2015. However, it did not document other important visitor's information identified within NIST, such as the visitor's signature and the need or reason for the visit, and the identity of CSB staff who escorted the visitor. The administrative assistant told us that she walked the visitors to the server room but there was no procedure established and she did not check to see if the visitor log was completed because the log was a new process and the server room door was previously left open due to an overheating problem. During our review, CSB indicated it updated the visitor log to comply with the latest NIST guidance.

Escorting Visitors: CSB did not have procedures in place to escort server room visitors and to monitor visitors' activities while in the server room. NIST requires that the visitors to the server room be escorted and their activities monitored. However, both of the two personnel who were listed as being assigned the keys to the server room indicated they did not escort visitors, ensure visitors completed the visitor log, or monitor visitors while they were accessing the server room. The CSB administrative assistant, who actually had the key to the server room, indicated that if she did not know the person, she walked the visitor to the server room, but did not stay and monitor the visitor while in the server room. Furthermore, she indicated that she did not escort and monitor the visitors because the door was previously left open and no procedures were established.

Key Security: CSB had not properly secured the keys to the server room. GSA issued three keys to CSB for the WRO server room door. We found the three keys were not secured and were accessible to all personnel in the WRO facility where the server room resides. The newly renovated WRO server room—the size of a small office closet—is accessible with a key lock, and may also serve as a utility closet as it contained electrical and phone panels, two folding step stools and a vacuum cleaner. The administrative assistant—the designated key holder—kept one key in her unlocked desk drawer. CSB kept the other two keys in an unlocked box inside the supply cabinet with a combination lock. All WRO employees knew the combination to the supply cabinet and could easily access the server room keys at any time. The administrative assistant said she used her key to open the server room for visitors. NIST requires that organizations secure keys, combinations and other physical access devices. To assist in more properly securing the physical access to the server room, CSB indicated it plans to install HSPD-12 PIV Card Access on the server room door.

Without these key physical controls in place, CSB cannot protect the WRO server room and critical data stored on the servers from unauthorized access. Our site visit noted that CSB does not use off-site storage for its server backup data, secure the WRO servers in lockable cabinets that prevent unauthorized personnel from tampering with the IT assets, or use a video surveillance recording system to track activity within the server room. As such, CSB finds itself at a disadvantage when performing investigations of server room physical security incidents, or preventing intentional destruction and pilfering of backup data.

Key Environmental Protection Controls Not in Place

CSB had not implemented key environmental protection controls to protect the WRO server room from environmental threats such as fire and humidity. NIST SP 800-53, Revision 4, requires that federal organization server rooms containing moderate sensitive data have automatic fire suppression capability and humidity controls within the server room, and water damage protection controls when applicable. However, WRO did not have these controls because there were no approved written environmental protection policy and procedures to guide CSB staff in protecting the WRO network equipment and important data stored on the servers against environmental threats. Furthermore, CSB had not taken steps to implement automatic fire suppression capability and humidity controls within the WRO server room. Details follow.

Automatic Fire Suppression: CSB did not have automatic fire suppression capability in place in the WRO server room. When WRO moved into the GSA's newly renovated facility, WRO did not ensure the server room was retrofitted for automatic fire suppression capability. CSB indicated that server backups are done remotely using mirrored disks located inside the server room and there is no off-site storage of servers' backups. NIST requires that federal organization server rooms have automatic fire suppression capability if the servers contain moderate sensitive data and the server room is not staffed on a continuous basis, as CSB indicated was the case here. In addition, CSB did not have smoke detectors, fire alarms or fire extinguishers inside the WRO server room, although it does have them located throughout the rest of the building.

Humidity Controls: CSB did not monitor humidity levels in the WRO server room. NIST requires federal organizations to maintain humidity at organization-defined acceptable levels and monitor humidity levels for fluctuations potentially harmful to the servers. The Chief Information Officer indicated that he intends to install a sensor and associated software that will monitor the humidity levels in the WRO server room.

Water Damage Protection Controls: CSB did not have water damage protection controls in the WRO server room. There was no current evidence of water leaks and there are currently no water pipes in the ceiling above the server room. However, if CSB installs a sprinkler system for fire suppression, NIST specifies that appropriate water damage protection controls be put in place to protect the network equipment and data from loss or damage due to water leakage. Examples of water damage protection controls are installing a master shutoff or isolation water valves that are accessible to key personnel to shut off the water supply if a leak occurs.

Without these key environmental controls in place, CSB cannot protect critical CSB network equipment and associated data critical to CSB investigations from loss or damage due to fire or humidity levels outside the acceptable range. In addition, water leakage could result in damage or data loss if applicable water protection controls are not employed with the fire suppression capability.

Recent CSB Action Prompted By OIG Work

CSB took action to improve physical and environmental controls at the WRO server room. During the course of our audit, CSB:

- Implemented processes to monitor temperature levels.
- Started using a visitor access log to monitor the room's access and revised the visitors log to comply with the latest NIST guidance.
- Installed software to enable automatic orderly shutdown of the WRO servers in the event of a power outage.

Conclusion

CSB WRO servers store all WRO investigative data critical to CSB investigations. In addition, the associated data backup is stored inside the server room. Critical CSB network equipment and associated investigative data may be susceptible to theft, loss or damage due to weak security controls over access to the server room or unexpected environmental disruptions.

Recommendations

We recommend that the Chairperson, U.S. Chemical Safety and Hazard Investigation Board:

1. Develop and implement written physical and environmental protection policy and procedures as required by NIST.

2. Develop, approve, maintain, review and update, as appropriate, a roster of individuals authorized to access the WRO server room.

3. Develop, maintain and enforce an access control process to document and monitor and log all physical access to the WRO server room.

4. Periodically review the physical access logs generated by the access control process, and the visitor access logs for suspicious physical access activities.

5. Escort and monitor activities of visitors (personnel not on the server room authorized access list) while in the WRO server room.

6. Develop and implement procedures to ensure server room keys are secured and available for use by only those individuals on the server room authorized access list.

7. Determine whether it is feasible to install automatic fire suppression capability and appropriate water damage protection controls in the WRO server room. If installing automatic fire suppression capability and appropriate water damage protection is not feasible, implement other risk mitigating strategies to reduce the WRO server risks to an acceptable level.

CSB Response and OIG Evaluation

The CSB stated that it takes information security seriously and works diligently each year to address the recommendations from the FISMA audits. The CSB stated it is working with GSA to install HSPD-12 card readers for the WRO. The CSB indicated it plans to establish an offsite backup procedure and identify a contractor or vendor to support its WRO offsite data backup efforts. The CSB also stated it has added a humidity sensor for the WRO server room.

The CSB agreed overall with our recommendations and provided planned corrective actions and milestones. For Recommendation 5, the CSB stated that it has started logging access of escorted visitors. The CSB also confirmed that it is currently escorting and monitoring the activities of visitors. Based on CSB's response and confirmation, we considered Recommendation 5 closed. We also revised Recommendation 7 since CSB indicated that it added humidity sensors and would evaluate the feasibility of installing fire suppression and water damage controls. The CSB and OIG agreed with the revisions to Recommendation 7. We agreed with the CSB's plan of corrective actions and estimated completion dates, and consider Recommendations 1, 2, 3, 4, 6 and 7 open with corrective actions pending.

Appendix A contains CSB's response to our draft report.

Chapter 3
Status of Prior-Year Audit Recommendations

We reviewed documentation related to the prior year's FISMA audit of CSB; and the CSB processes, procedures and other provided documentation to assess the implementation status of CSB corrective actions taken to address prior-year recommendations. This involved following up on the 17 information system security recommendations in Report No. 15-P-0073, *Key Aspects of CSB Information Security Program Need Improvement*, dated February 3, 2015. These recommendations related to CSB's system security plan, risk management framework, visitor access records, risk of unimplemented privacy and security controls and known vulnerabilities, orderly shutdown of IT assets, and asset inventory.

CSB has made progress in completing the agreed-to corrective actions for 13 of the 17 prior-year recommendations. We consider the remaining four recommendations open because CSB had not provided documentation to support actions it took to address each of the recommendations. We did not assess the effectiveness of CSB's actions because the agency had just completed implementation of many of the corrective actions during our field work. The status of issues from prior recommendations with corrective actions that are not complete are listed in the following table.

Table 1: Status of four open prior audit recommendations

Recommendation	CSB's agreed-to corrective actions that need completing
1. Update the GSS [general support system] SSP [system security plan] to be compliant with the latest NIST guidance on privacy and information security controls for federal systems.	CSB agreed to update the GSS SSP by March 30, 2015. CSB provided its SSP, dated June 2015. Although CSB updated the SSP, we noticed CSB did not use the correct NIST nomenclature when it labeled or categorized information system as "Medium." (The correct NIST nomenclature is "Moderate.") Also, CSB did not identify specific NIST SP 800-53 security controls it evaluated (in the table at the end of its SSP, the last two pages, in the fourth column heading, "Controls Evaluated") for the following security controls: the last six of "System and Communications Protection" and all 11 of "System and Information Integrity" controls. It appears that CSB incorrectly identified priority codes "P1" or "P2" instead of control numbers for "SC-20" to "SC-39" and "SI-1" to "SI-16." In addition, while the SSP lists the other controls specified in NIST 800-53, Revision 4, for a system that contains moderate-risk data, the SSP does not detail (as specified by NIST): how each of the security controls is implemented, terms and conditions CSB used to select each of the appropriate security controls to achieve adequate security for its information systems, and the personnel responsible for implementing each of the security controls.

Recommendation	CSB’s agreed-to corrective actions that need completing
2. Create a policy and procedure that requires that all CSB information SSPs are to be reviewed annually and updated based on changes to federal guidance.	CSB agreed to finalize Risk Management Framework [RMF] policy and procedure by March 30, 2015. Although CSB developed an RMF, as of our cutoff date (August 3, 2015), the RMF was not formally approved and published.
4. Develop and implement an RMF for continuous monitoring of CSB information systems.	CSB agreed to implement RMF policy and procedure by March 30, 2015. Although CSB developed an RMF, as of our cutoff date (August 3, 2015), the RMF was not formally approved and published.
6. Require the Authorizing Official to reauthorize the GSS SSP to formally accept the risks for all federally required unimplemented privacy and information security controls.	CSB agreed to finalize RMF policy and procedure by March 30, 2015. CSB reauthorized its GSS to operate and developed an RMF strategy. However, as of our audit field work cutoff date of August 3, 2015, management had not formally approved and published the RMF.

Source: OIG analysis.

CSB Response and OIG Evaluation

The CSB planned to update and reissue the Certification and Accreditation package and finalize RMF policy and procedures to address the above prior-year audit recommendations. We agree with the CSB’s response and its planned corrective actions and estimated completion dates, and consider our prior-year recommendations open until completion of corrective actions.

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	8	Develop and implement written physical and environmental protection policy and procedures as required by NIST.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	1/30/16		
2	8	Develop, approve, maintain, review and update, as appropriate, a roster of individuals authorized to access the WRO server room.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	1/30/16		
3	8	Develop, maintain and enforce an access control process to document and monitor and log all physical access to the WRO server room.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/16		
4	8	Periodically review the physical access logs generated by the access control process, and the visitor access logs for suspicious physical access activities.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/16		
5	8	Escort and monitor activities of visitors (personnel not on the server room authorized access list) while in the WRO server room.	C	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	10/16/15		
6	8	Develop and implement procedures to ensure server room keys are secured and available for use by only those individuals on the server room authorized access list.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/16		
7	8	Determine whether it is feasible to install automatic fire suppression capability and appropriate water damage protection controls in the WRO server room. If installing automatic fire suppression capability and appropriate water damage protection is not feasible, implement other risk mitigating strategies to reduce the WRO server risks to an acceptable level.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/16		

[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

CSB Response to Draft Report

U.S. Chemical Safety and Hazard Investigation Board

1750 Pennsylvania Avenue NW, Suite 910 | Washington, DC 20006
Phone: (202) 261-7600 | Fax: (202) 261-7650
www.csb.gov

Vanessa Allen Sutherland
Chairperson and Member

Manny Ehrlich, Jr.
Board Member

Rick Engler
Board Member

Kristen M. Kulinowski, Ph.D.
Board Member

October 16, 2015

Rudy Brevard
Director, IRM Audits
U.S. Environmental Protection Agency
Office of Inspector General
1200 Pennsylvania Ave
Washington, DC 20460

Dear Mr. Brevard:

Thank you for the opportunity to review and comment on the draft report of CSB's compliance with the Federal Information Security Management Act (FISMA) for fiscal year 2015.

The CSB takes information security seriously and works diligently each year to address the recommendations from the FISMA audits. The CSB agrees overall with the findings and recommendations from this most recent report; however, the following is a brief background on the CSB's planned actions in response to these recommendations.

CSB WRO Server Room Lacks Key Physical and Environmental Controls

Key Physical Controls Not in Place

Authorized access: A policy governing access and designating approved individuals for access to the WRO server room will be written, approved by CSB management, and posted on the CSB Sharepoint site.

Physical access logs/visitor logs: The CSB improved the WRO server room visitor log in keeping with the OIG's recommendations. The written log posted on the server room door is used to record the visitor's name, agency, form of identification, date and time in, date and time out, reason for visit, and CSB escort. All entries to the server room by non-CSB personnel are now logged on the new form.

Escorting visitors: Visitors are to be escorted by designated personnel, and escorts are recorded on the improved visitor log.

Key security: The CSB is working with GSA to install HSPD-12 card readers in three locations: the two entry doors to Building 21B and the server room door. Once installed, this will take the place of key entry to the server room. The HSPD-12 card reader will also, as it does at headquarters, govern who has access to the server room and maintain a log of who unlocks the door and when. This will be a more accurate means of determining whose card was used to open the door in the event of any suspicious activity or physical security incidents.

Offsite Backups: The CSB is also working to establish an offsite backup procedure for the WRO server data similar to that in place at headquarters. We are working to identify a contractor or vendor to pick up and deliver hard drives containing essential backup data on a regular (such as biweekly) basis.

Key Environmental Protection Controls Not in Place

Automatic fire suppression: Automatic fire suppression capability was not installed in Building 21 when the CSB moved in. The CSB will give consideration to installing fire suppression controls based on the cost and complexity and will decide whether to move ahead with installation or implement other risk mitigating strategies to give a determination of acceptable risk.

Humidity controls: A humidity sensor has been added to the NTI Enviromux temperature and humidity sensor in the WRO server room. The sensor is configured to send email alerts to CSB IT staff in the event of a humidity reading outside the normal range. Both the headquarters and WRO sensors are now configured this way.

Water damage protection controls: Water damage protection capability was not installed in Building 21 when the CSB moved in. The CSB will give consideration to installing water damage controls based on the cost and complexity and will decide whether to move ahead with installation or implement other risk mitigating strategies to give a determination of acceptable risk.

Status of Prior-Year Audit Recommendations

The remaining prior-year audit recommendations will be addressed, and closed, with the reissuance of an updated Certification and Accreditation package signed by me, to replace the one issued under the signature of the Board Member Delegated Interim Executive and Administrative Authority. The revised and updated C&A will include a formally approved and published risk management framework (RMF) policy.

Plan of Actions and Milestones

The attached table summarizes CSB's plan of action for each recommendation.

If you or your staff have any questions about this response, please feel free to contact our CIO, Charlie Bryant, at 202-261-7666.

Sincerely,

Vanessa Allen Sutherland
Chairperson and Board Member

Number	Recommendation	Planned/Completed Action
2014-01	Update the GSS SSP to be compliant with the latest NIST guidance on privacy and information security controls for federal systems.	By January 30, 2016: Update and reissue C&A package
2014-02	Create a policy and procedure that requires that all CSB information SSPs are to be reviewed annually and updated based on changes to federal guidance.	By January 30, 2016: Finalize RMF policy and procedure and include with updated C&A package
2014-04	Develop and implement a risk management framework for continuous monitoring of CSB information systems.	By January 30, 2016: Finalize RMF policy and procedure and include with updated C&A package
2014-06	Require the Authoring Official to reauthorize the GSS SSP to formally accept the risks for all federally required unimplemented privacy and information security controls.	By January 30, 2016: Update and reissue C&A package
2015-01	Develop and implement written physical and environmental protection policy and procedures as required by NIST.	By January 30, 2016: Develop and approve such policy and procedures
2015-02	Develop, approve, maintain, review and update, as appropriate, a roster of individuals authorized to access the WRO server room.	By January 30, 2016: Create and approve a roster of authorized individuals
2015-03	Develop, maintain and enforce an access control process to document and monitor and log all physical access to the WRO server room.	By March 30, 2016: Create a written process describing physical access, dependent on implementation of HSPD-12 card reader access
2015-04	Periodically review the physical access logs generated by the access control process, and the visitor access logs for suspicious physical access activities.	By March 30, 2016: Review physical access logs, also dependent on implementation of HSPD-12 card reader access
2015-05	Escort and monitor activities of visitors (personnel not on the server room authorized access list) while in the WRO server room.	Immediately: Log access of escorted visitors, as recorded on physical access log
2015-06	Develop and implement procedures to ensure server room keys are secured and available for use by only those individuals on the server room authorized access list.	By March 30, 2016: Develop and approve a written policy and procedure outlining server room key security and access. Also dependent on implementation of HSPD-12 card reader access

2015-07	Install automatic fire suppression capability, humidity controls and appropriate water damage protection controls in the WRO server room.	By March 30, 2016: We will have evaluated the feasibility of installing fire suppression and water damage controls.

Appendix B

Distribution

Chairperson and Chief Executive Officer, U.S. Chemical Safety and Hazard Investigation Board
Board Members, U.S. Chemical Safety and Hazard Investigation Board
Chief Information Officer, U.S. Chemical Safety and Hazard Investigation Board
Deputy Chief Information Officer, U.S. Chemical Safety and Hazard Investigation Board
Director of Administration and Audit Liaison, U.S. Chemical Safety and Hazard Investigation Board
Deputy Director of Administration, U.S. Chemical Safety and Hazard Investigation Board