



U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL



U.S. Chemical Safety Board

Key Aspects of CSB Information Security Program Need Improvement

Report No. 15-P-0073

February 3, 2015



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

Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Eric K. Jackson Jr.
Christina Nelson

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act of 2002
GSS	General Support System
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMF	Risk Management Framework
SSP	System Security Plan

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

More information at www.epa.gov/oig/hotline.html.

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](#)



At a Glance

Why We Did This Review

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act of 2002 (FISMA).

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. The Inspector General is to perform an annual independent evaluation of the security program.

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.

The full report is at: www.epa.gov/oig/reports/2015/20150203-15-P-0073.pdf

Key Aspects of CSB Information Security Program Need Improvement

What We Found

CSB should improve key aspects of its information security program to better manage practices related to information security planning, physical and environmental security controls, its vulnerability testing process, and internal controls over its information technology inventory.

CSB's ability to increase its situational awareness and reduce risk exposure is challenged by its lack of a real-time continuous monitoring strategy.

The National Institute of Standards and Technology provides guidance for how federal organizations should continuously monitor security control effectiveness and remediate vulnerabilities. Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, provides guidance on how federal programs should develop internal controls to ensure that they achieve their desired objectives.

Federal information systems are subject to threats, including environmental disruptions, human and/or machine errors, and purposeful attacks. If CSB information technology inventory is stolen or its network breached, CSB data, information and configurations may be exposed.

Recommendations and Planned CSB Corrective Actions

We recommend that CSB update and maintain its system security plan, implement a risk management framework, create a visitor access record for the server room, formally accept risk of unimplemented privacy and security controls and vulnerabilities, and develop a process for orderly shutdown of critical information technology assets. We also recommend that CSB create plans to remediate systems with known vulnerabilities and expand its monthly vulnerability testing process to include all assets attached to the network. Further, we recommend that CSB improve its inventory control practices to ensure personnel do not perform incompatible duties, provide policies and procedures for safeguarding inventory, review and document lost items, and recover costs for lost items due to employee negligence.

CSB concurred with our recommendations and provided corrective actions with estimated completion dates for each recommendation. All 17 recommendations we made are resolved and corrective actions are completed or ongoing.

Noteworthy Achievements

CSB took significant action to implement processes to eliminate excessive electronic device inventory and to document management's justification for assigning multiple electronic devices to certain CSB personnel.



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

THE INSPECTOR GENERAL

February 3, 2015

The Honorable Rafael Moure-Eraso, Ph.D.
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
2175 K Street, NW, Suite 400
Washington, DC 20037-1809

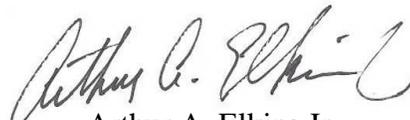
Dear Dr. Moure-Eraso:

This is our report conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency. This report represents our final position on our review of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of the Federal Information Security Management Act. The report contains findings that describe the issues 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 CSB position. CSB managers will make the final determinations on matters in this report.

In responding to the draft report, CSB concurred with all recommendations and provided corrective actions to address each recommendation.

We will post this report and CSB's response to the report on our website at <http://www.epa.gov/oig>.

Sincerely,



Arthur A. Elkins Jr.

Table of Contents

Chapters

1	Introduction	1
	Purpose	1
	Background.....	1
	Responsible Offices	2
	Scope and Methodology	2
	Noteworthy Achievements	3
2	Improvements Needed in CSB’s Information Security Planning	4
	Incomplete System Security Plan.....	4
	Unimplemented Risk Management Framework.....	5
	Conclusions	5
	Recommendations	6
	CSB Response and OIG Evaluation	6
3	Improvements Needed in CSB’s Server Room Security Controls	7
	Server Room Lacks Visitor Access Record	7
	CSB Lacks Capability to Perform Orderly Shutdown of Critical IT Assets ..	7
	Conclusions	8
	Recommendations	8
	CSB Response and OIG Evaluation	8
4	Known Vulnerabilities Threaten Security of CSB’s Network	10
	Known Vulnerabilities Not Remediated	10
	Network-Connected Devices Not Tested	11
	Conclusions	11
	Recommendations	11
	CSB Response and OIG Evaluation	12
5	Improvements Needed Over IT Assets Inventory	13
	Segregation of Duties Lacking	13
	Controls Needed to Prevent Lost Inventory	13
	Conclusions	14
	Recommendations	14
	CSB Response and OIG Evaluation	15
	Status of Recommendations and Potential Monetary Benefits	16

Appendices

A	CSB’s Response to Draft Report	18
B	Distribution	22

Chapter 1

Introduction

Purpose

The Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) conducted this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act of 2002 (FISMA) for fiscal year 2014.

Background

CSB is authorized by the Clean Air Act Amendments of 1990 and became operational in January 1998. CSB is an independent federal agency charged with investigating root causes for industrial chemical accidents. CSB does not issue fines or citations, but does make recommendations to plants, regulatory agencies such as the Occupational Safety and Health Administration and the EPA, industry organizations, and labor groups. During fiscal year 2014, CSB's personnel included 40 employees. CSB's investigative staff includes chemical and mechanical engineers, industrial safety experts, and other specialists with experience in the private and public sectors. The majority of CSB's staff are stationed at its headquarters in Washington, D.C. The CSB also has a Western Regional Office of Investigations, located in Denver, Colorado.

Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General and is supported by security policy promulgated through the Office of Management and Budget (OMB) and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard and Special Publication series.

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. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, practices and compliance with FISMA.

In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices, and to report the evaluation results to OMB.

FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

Responsible Offices

Within CSB's Office of Administration are CSB personnel responsible for CSB's information technology (IT) security program. The Director of Information Technology and the Chief Information Officer are responsible for making risk management decisions regarding deficiencies, and their potential impact on controls and the confidentiality, integrity and availability of systems. CSB management is responsible, based on its risk management decisions, to implement solutions that are appropriate for CSB's IT environment for its headquarters office in Washington, D.C., and its Western Regional Office of Investigations in Denver.

Scope and Methodology

We conducted our audit from June to October 2014 at CSB headquarters in Washington, D.C. We performed this 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 conclusions based on our audit objective.

We assessed CSB's compliance, implementation and effectiveness over the following FISMA micro agency reporting metrics: system inventory, asset management, vulnerability and weakness management, and identity and access management. The remaining metrics will be evaluated on a rotational basis during future CSB FISMA audits. In addition, we also reviewed CSB server room physical security and environmental controls as well as CSB IT security processes, procedures and other documentation against guidance provided by NIST.

We reviewed CSB's internal control processes over its IT asset inventory. We selected a random sample of CSB assigned inventory to verify the inventory listing and reconciliations performed by CSB inventory control officers.

We performed technical vulnerability testing at the CSB headquarters office in July 2014. We tested all Internet Protocol addresses associated with CSB's networked resources located at CSB headquarters and the Western Regional

Office of Investigations. The purpose of this testing was to identify the existence of commonly known technical vulnerabilities using a commercially available network vulnerability assessment tool recognized by NIST. We did not attempt to penetrate any system or device, or try to gain access to other network resources using the identified vulnerabilities. We used the risk rating provided by the network vulnerability assessment tool to determine the level of harm each vulnerability could cause to a network resource.

We had no prior report recommendations to follow up on during this audit.

Noteworthy Achievements

CSB has taken significant action to implement processes to eliminate excess electronic device inventory and to document management justification for CSB personnel assigned multiple electronic devices. CSB Inventory Control Officers review inventory for excess electronic items and annually dispose of excess electronic inventory items through a General Services Administration-approved recycler. CSB's Physical Inventory Guidelines also include a CSB Device Justification form that CSB management uses to describe its decision for assigning multiple computer and mobile devices to a CSB employee.

Chapter 2

Improvements Needed in CSB's Information Security Planning

CSB lacks a system security plan (SSP) that contains all the required information needed to authorize its systems to operate. CSB has yet to implement the NIST Risk Management Framework (RMF) for Federal Information Systems. Federal guidance requires organizations to describe how they implement security controls for federal systems and to make this information available to the individual that will authorize the system to operate. Federal guidance outlines the six-step RMF process organizations are to follow to continuously monitor IT systems and networks. CSB security planning documents are incomplete because CSB lacks processes to review and update the required information on an annual basis or as major changes to the federal guidance occur. CSB also has not finalized its plans for how it would implement the RMF. Updated data on implemented security controls and an effectively implemented RMF are key to driving management decisions on what is critical in protecting the network. Without complete information, the Authorizing Official—the person formally assuming responsibility for the organization's risks—could potentially make decisions to operate the network that are outside the organization's risk tolerance or that can be detrimental to the organization accomplishing its mission.

Incomplete System Security Plan

CSB's General Support System (GSS) SSP is incomplete since it does not include all the required security control baselines for a moderate information system. Specifically, CSB's GSS SSP does not include nine security controls and 24 security control enhancements as required by NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, for a system that contains moderate-risk data. CSB's GSS SSP also does not detail: how security controls are implemented, terms and conditions CSB used to select the appropriate security controls to achieve adequate security for its information systems, and personnel responsible for implementing the security controls.

CSB reviews its system security planning documentation every 3 years or more frequently based on significant changes. However, the CSB IT Department Standard Operating Procedure does not consider updates to federal guidance as a significant change that would require CSB management to review and update its information system security documentation. Since CSB's last review of its GSS SSP, NIST Special Publication 800-53 was revised and security controls and control enhancements have been added and withdrawn for low, moderate and high baselines.

According to NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, SSPs should be reviewed and updated at least annually to ensure the information system status, functionality and design; and that the plan reflects the correct information about the system.

Federal information systems are subject to threats, including environmental disruptions, human or machine errors, and purposeful attacks. CSB risks being unable to effectively mitigate security vulnerabilities and protect the organization's resources and data from undue harm by using outdated security controls. Furthermore, federal guidance states that management's Authorizing Official authorization of information systems should be based on an assessment of management, operational and technical controls. Without providing the Authorizing Official with complete and up-to-date information, this person would be making uninformed decisions on whether to operate the system in its current state. This could ultimately result in the Authorizing Official deciding to operate a system (1) outside of the organization's risk tolerance, (2) with the opportunity to direct that personnel remediate weaknesses that senior agency officials deem important, or (3) with weaknesses that are detrimental to the organization accomplishing its mission.

Unimplemented Risk Management Framework

CSB has not finalized a strategy to transition from a 3-year certification and authorization process to an RMF for continuously monitoring CSB's information systems. NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, requires federal organizations to transform their traditional, static, procedural certification and authorization process to a dynamic six-step RMF process. CSB has begun developing an RMF strategy, but CSB management has not yet fully implemented the strategy within CSB's IT environment.

By using an RMF strategy, CSB's management can effectively manage information system security risks to be consistent with the organization's mission, support ongoing security authorization decisions, and implement appropriate risk mitigation strategies. Without a codified effective continuous monitoring strategy in place, CSB inhibits its ability to gather the real-time status of its data, network, end points, and cloud devices and applications, thereby reducing its situational awareness and increasing its risk exposure.

Conclusions

The lack of up-to-date information on security controls and the lack of processes to conduct real-time monitoring of CSB's network inhibits management's ability to make risk-based decisions to continuously authorize CSB's network and to effectively combat cyber threats.

Recommendations

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

1. Update the GSS SSP to be compliant with the latest NIST guidance on privacy and information security controls for federal systems.
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.
3. Perform an annual review of all CSB information SSPs and document the review.
4. Develop and implement an RMF for continuous monitoring of CSB information systems.

CSB Response and OIG Evaluation

In its response to our draft audit report, CSB agreed with our recommendations and provided corrective actions with estimated completion dates. We consider the recommendations open with corrective actions pending.

Subsequent to the issuance of our draft report, we met with CSB officials to discuss their concerns with the draft report. Where appropriate, we modified the report language to address management's concerns.

Chapter 3

Improvements Needed in CSB's Server Room Security Controls

CSB has not implemented key physical security controls necessary to track visitors to its server room or mitigate loss of data due to a power failure. Federal guidance requires that federal organizations develop, implement, assess, authorize and continuously monitor security controls. However, the CSB server room does not have a visitor access record or a strategy for an orderly shutdown of servers during non-business hours. As a result, critical CSB IT equipment and associated data may be susceptible to damage and/or loss due to untracked visitors to the server room or unexpected power disruptions.

Server Room Lacks Visitor Access Record

CSB does not maintain a visitor access record to identify and track visitors and/or non-IT CSB personnel entering the server room. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, Monitoring Physical Access Security Control PE-8, states that an organization should maintain and review visitor access records.

CSB representatives did not believe that a visitor access record was necessary because (1) the server room is off-limits to non-IT CSB personnel, (2) the server room is protected with two cipher locks, and (3) infrequent visitors to the server room are always accompanied by CSB IT personnel. During fieldwork, CSB representatives indicated that the organization accepts the risk of not keeping a visitor access record. However, management's acceptance of the risk is not documented in its GSS SSP. Furthermore, the organization's Authorizing Official—the individual who accepts the risks for operating information systems without controls in place—has not officially approved an authorization to operate with this risk noted. If the server room is tampered with, the lack of server room visitor access records inhibits CSB's ability to determine dates, times and names of potential perpetrators. Prior to the issuance of the final report, CSB indicated that a visitor log had been added to both the Washington and Denver server rooms.

CSB Lacks Capability to Perform Orderly Shutdown of Critical IT Assets

CSB IT critical assets support all CSB servers for CSB headquarters and the Western Regional Office of Investigations. These servers could contain personal identifiable information and other sensitive or confidential data. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, Emergency Power Security Control PE-11, states that an organization should provide a short-term Uninterruptable

Power Supply to facilitate an orderly shutdown of the information system in the event of a loss of power from the primary power source.

CSB representatives stated that they do not have controls in place or have a documented strategy to ensure an orderly shutdown of critical IT assets in the event of power loss during non-business hours. We noted that CSB servers receive emergency back-up power from Uninterruptable Power Supplies located in the server room. According to CSB representatives, the Uninterruptable Power Supplies provide approximately 15 minutes of back-up power and CSB has not configured the Uninterruptable Power Supplies to automatically shut down critical assets. As such, in the event of a power loss, there would not be sufficient time for the IT staff to perform an orderly shutdown of the servers unless they were in the server room or reasonably close by the CSB building.

CSB stated it performs regular backups of the server information. However, if servers undergo an abnormal shutdown, CSB may lose up to 2 weeks of data and/or CSB's critical IT equipment may become damaged.

Conclusions

Since CSB headquarters' servers store all of CSB headquarters and regional investigation data, which may contain personal identifiable information and other sensitive or confidential data, CSB must protect its servers from damage by power loss or tampering by undocumented visitors.

Recommendations

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

5. Create a visitor access record for the server room or document the acceptance of the risk in the GSS SSP.
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.
7. Develop and implement a strategy to be able to conduct an orderly shutdown of CSB servers in the event of a power outage when IT personnel are not present.

CSB Response and OIG Evaluation

In its response to our draft audit report, CSB agreed with our recommendations and provided corrective actions with estimated completion dates. CSB indicated that corrective actions have been completed for Recommendation 5. The OIG thus

considers Recommendation 5 to be closed and the other recommendations open with corrective actions pending.

Subsequent to the issuance of our draft report, we met with CSB officials to discuss their concerns with the draft report. Where appropriate, we modified the report language to address management's concerns.

Chapter 4

Known Vulnerabilities Threaten Security of CSB's Network

CSB's network contained multiple high-risk and medium-risk vulnerabilities. These vulnerabilities were identified on network-connected IT assets at CSB headquarters and the Western Region Office. Federal guidance requires organizations to assess the security posture, continually monitor information systems, and identify and remediate vulnerabilities. CSB has not remediated or identified many of the noted vulnerabilities. This is because CSB had not made plans to replace assets it knew had vulnerabilities, and because CSB expanded its regular vulnerability testing program to include all assets attached to the CSB network. As a result, CSB's network continues to be susceptible to attack by (1) known weaknesses that, if exploited, could cause significant harm to CSB; and (2) unmonitored assets connected to the network that could be used as launching points to attack other known vulnerable systems or to remove data from CSB.

Known Vulnerabilities Not Remediated

CSB indicated that it knew about the existence of several of the vulnerabilities identified during our technical vulnerability testing. CSB had identified the same vulnerabilities as a result of its regular vulnerability testing program and recorded the vulnerabilities within the organization's Vulnerability Management Exception Log. However, CSB had not prioritized the remediation of these vulnerabilities. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, Vulnerability Scanning Security Control RA-5, states organizations need to remediate legitimate vulnerabilities in accordance with an organizational assessment of risk and share information obtained from the vulnerability scanning process to help eliminate similar vulnerabilities in other information systems.

We noted that CSB is proactive and diligent in identifying and cataloging its known vulnerabilities. CSB stated that systems with known vulnerabilities cannot be remediated due to the lack of newer software available for the affected systems or the lack of newer software that is compatible with the existing systems' configurations. However, CSB had not created plans of actions and milestones to plan remediation activities to reduce or eliminate the known vulnerabilities as required by NIST Special Publication 800-53.

By not developing a strategy for remediating vulnerabilities, these known weaknesses will continue to pose risks to CSB's network without an end date when the organization can start focusing its limited resources on other critical information security activities. By creating plans of action and milestones, CSB would be in a better position to justify its security control investments and could

use this information to help prioritize the necessary corrective actions for its vulnerable systems.

Network-Connected Devices Not Tested

CSB does not test all IT assets attached to its network. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, Vulnerability Scanning Security Control RA-5, specifies that organizations are required to ensure networked devices—including printers, scanners and copiers—are included in the agency's vulnerability tests.

CSB procedures require it to conduct regular vulnerability testing of its network. Even though CSB's vulnerability testing methodology includes testing network appliances as part of its scope for testing, CSB's vulnerability testing methodology does not include testing printers or multi-functioning devices connected to the network. These types of devices typically contain central processing units and storage media, which would allow the devices to function as computers. These devices are known to have multiple vulnerabilities and have been identified as potential targets for launching attacks against an organization's network. By not regularly testing these types of devices for vulnerabilities and remediating them, CSB potentially leaves its network vulnerable to attack. As such, an attacker could take control of one of these devices and use it to cause significant harm to CSB's systems and data. Remediating vulnerabilities on these types of devices reduces CSB's exposure to network attacks.

Conclusions

CSB's network is at risk of attack due to known weaknesses existing without defined plans to remediate them, and because IT assets connected to the network have not been tested for vulnerabilities. The combination of these two weaknesses could potentially create a situation where untested IT assets could be used as a staging area to (1) conduct attacks against known vulnerable CSB systems or (2) remove data from CSB without detection.

Recommendations

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

8. Create plans of action and milestones for when CSB would either update or replace all systems with known vulnerabilities.
9. Update the GSS SSP and have the authorizing official formally accept the risks of operating systems with known vulnerabilities when the organization made a risk-based decision to accept the risks.

10. Update the organization's vulnerability testing methodology to test all devices connected to the network. This should include all printers and multifunctioning devices.

CSB Response and OIG Evaluation

In its response to our draft audit report, CSB agreed with our recommendations and provided corrective actions with estimated completion dates. CSB indicated that corrective action has been completed for Recommendation 10. The OIG thus considers Recommendation 10 to be closed and the other recommendations open with corrective actions pending.

Chapter 5

Improvements Needed Over IT Assets Inventory

CSB lacks segregation of duties internal controls to protect its inventory, and has no process in place for recovering costs for inventory lost due to employee neglect. OMB guidance requires the agency head to establish internal control systems to safeguard assets from waste, loss, unauthorized use or misappropriation. CSB neither implemented controls to ensure personnel do not perform incompatible duties nor established processes to investigate or recover the cost of inventory potentially lost due to employee neglect. As a result, CSB's inventory is subject to misappropriation without detection or means to recover the cost of items lost due to negligence.

Segregation of Duties Lacking

CSB had not segregated the duties for maintaining its IT inventory. For instance, CSB has one employee serving as the Lead Inventory Control Officer, IT Inventory Control Officer and Inventory System Database Administrator. This allows the employee to enter, alter and delete information from the inventory system database without independent oversight. OMB Circular A-123, *Management's Responsibility for Internal Control*, requires the agency head to implement control activities to ensure that accountability over assets are safeguarded against waste, loss, unauthorized use or misappropriation.

CSB's IT assets may be misappropriated without detection due to CSB's lack of compensating controls to ensure personnel do not perform incompatible duties. While it is common for a small organization to have employees sharing various duties and responsibilities, it is prudent to have compensating controls in place to prevent opportunities for unauthorized or unintentional modification of the inventory records. Since one CSB employee simultaneously manages all IT assets and has the ability to add, edit and delete any inventory records from the system database, CSB management limits its ability to detect theft activity.

Controls Needed to Prevent Lost Inventory

Improvements are needed to determine whether lost CSB property inventory is due to employee negligence. CSB's current process for maintenance allows for lost items to remain indefinitely in the inventory system. Over the past 10 years, 8 percent of CSB's inventories (87 out of 1,145 inventory items) were assigned to lost departments. These 87 lost inventory items include:

- 3 iPhone 5s.
- 3 Laptops.
- 24 Digital Cameras.

- 21 Voice Recorders.
- 3 Government-Issued PIV Identification Cards.

According to OMB Circular A-123, management is responsible for designing internal controls to ensure assets are safeguarded against waste, loss, and unauthorized use or misappropriation.

Although CSB has written procedures that require personnel to conduct an annual physical inventory, CSB has not developed a method for investigating and making a determination as to whether lost items were due to employee negligence. If these items were lost due to employee negligence, CSB lacks policies and procedures for recovering the cost of the lost item from the employee.

Internal controls over property accountability are the cornerstone for safeguarding government assets. By not having processes to determine when items were lost due to employee negligence, CSB creates the environment where employees may not exercise reasonable due care when using government property because there are no consequences for not safeguarding the asset and returning the asset to the organization. By implementing processes to recover costs due to employee negligence, CSB sets the tone that management takes property accountability seriously and that employees are accountable for their actions.

Conclusions

CSB IT property is susceptible to potential misappropriation without putting in place controls to detect errors in property record-keeping or hold employees accountable for safeguarding assets in their possession.

Recommendations

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

11. Implement processes where employees are not performing incompatible property accountability duties.
12. Implement compensating controls to mitigate the risks for having one employee responsible for entering, altering and deleting information within the CSB inventory system without detection, if segregating the property accountability duties are not possible.
13. Develop and implement policies and procedures for safeguarding inventory from waste, loss, unauthorized use or misappropriation.
14. Conduct a review of all items recorded as lost within the CSB inventory system and make a determination regarding the status of the items.

15. Initiate actions to recover the costs for lost items if CSB determines the items were lost due to employee negligence.
16. Update the CSB inventory system with a description for the items designated as lost.
17. Make a determination as to whether lost items should be removed from the CSB inventory system.

CSB Response and OIG Evaluation

In its response to our draft audit report, CSB agreed with our recommendations and provided corrective actions with estimated completion dates. We consider the recommendations open with corrective actions pending.

Subsequent to the issuance of our draft report, we met with CSB officials to discuss their concerns with the draft report. Where appropriate, we modified the report language to address management's concerns.

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	6	Update the GSS SSP to be compliant with the latest NIST guidance on privacy and information security controls for federal systems.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
2	6	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.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
3	6	Perform an annual review of all CSB information SSPs and document the review.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
4	6	Develop and implement an RMF for continuous monitoring of CSB information systems.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
5	8	Create a visitor access record for the server room or document the acceptance of the risk in the GSS SSP.	C	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	12/1/14		
6	8	Require the Authorizing Official to reauthorize the GSS SSP to formally accept the risks for all federally required unimplemented privacy and information security controls.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
7	8	Develop and implement a strategy to be able to conduct an orderly shutdown of CSB servers in the event of a power outage when IT personnel are not present.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
8	11	Create plans of action and milestones for when CSB would either update or replace all systems with known vulnerabilities.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
9	11	Update the GSS SSP and have the authorizing official formally accept the risks of operating systems with known vulnerabilities when the organization made a risk-based decision to accept the risks.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	3/30/15		
10	12	Update the organization's vulnerability testing methodology to test all devices connected to the network. This should include all printers and multifunctioning devices.	C	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	12/1/14		
11	14	Implement processes where employees are not performing incompatible property accountability duties.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in \$000s)	
Rec. No.	Page No.	Subject	Status ¹	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
12	14	Implement compensating controls to mitigate the risks for having one employee responsible for entering, altering and deleting information within the CSB inventory system without detection, if segregating the property accountability duties are not possible.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
13	14	Develop and implement policies and procedures for safeguarding inventory from waste, loss, unauthorized use or misappropriation.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
14	14	Conduct a review of all items recorded as lost within the CSB inventory system and make a determination regarding the status of the items.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
15	15	Initiate actions to recover the costs for lost items if CSB determines the items were lost due to employee negligence.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
16	15	Update the CSB inventory system with a description for the items designated as lost.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		
17	15	Make a determination as to whether lost items should be removed from the CSB inventory system.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	6/1/15		

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.

CSB's Response to Draft Report

December 1, 2014

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 on the CSB's compliance with the Federal Information Security Management Act (FISMA) for fiscal year 2014.

The CSB takes information security weaknesses seriously and works diligently each year to address the recommendations from the FISMA audits. While the CSB agrees overall with the findings and recommendations from this most recent report, the following is a detailed discussion of our concerns (grouped by chapter title), which we hope you will take into consideration.

Improvements Needed in CSB's Information Security Planning

The report states that "CSB representatives indicated they have started to develop some aspects of the organization's RMF strategy." As part of the documentation submitted during the audit, the CSB provided a full draft Risk Management Framework (RMF) program document which we are in the process of implementing. Indeed, many of the recommendations from this section of the report are addressed in this program document. Consequently, we believe the background for this finding understates the current status of the CSB's work towards full compliance.

Nevertheless, the agency certainly agrees with the importance of implementing this program and associated documentation, and will be working as quickly as possible to address these issues. Please find our plan of action and milestones attached.

Improvements Needed in CSB's Server Room Security Controls

The report states that CSB "did not believe that a visitor access record was necessary because non-IT CSB personnel do not frequently visit the CSB server room" The CSB server room is in fact off limits to non-IT personnel. It is kept locked behind a cipher lock door 24/7 and is inaccessible to non-IT staff without a member of the IT staff present. The agency misinterpreted this to be a control enhancement over the security control; however, we now understand this to be insufficient. Consequently, we have added a visitor log to these rooms, as noted in the attached POA&M.

Known Vulnerabilities Threaten the Security of CSB's Network

The CSB will be working diligently to appropriately detail vulnerabilities in the Plan of Action and Milestones, as recommended in the draft report, and has already made a change to regularly scan all devices, including printers.

Improvements Needed Over IT Assets Inventory

The report mentions approximately 90 missing items in the inventory system; however, it makes no mention of the 10-year time period over which these items were lost. One of the items, for instance, was a Nikon digital camera stolen in the fall of 2004. Without this detail, the reader may assume that these items went missing in the course of one year which would certainly be indicative of a problem.

The report also states that the property inventory reports list eight (8) percent of the organization's inventory as lost. Since we don't purge the inventory of lost items, but do de-inventory obsolete/surplus items every year, this percentage is misleading. If this analysis factored in all the equipment we de-inventoried as well, the percentage of lost items in the database would indeed be much lower.

The conclusion that CSB's IT property is "highly susceptible" to potential misappropriation appears overstated given the level of lost devices in a 10-year period. We agree with the recommendations and are working to address these issues and improve our inventory program.

The attached table summarizes CSB's plan of action for each recommendation. As you will note, the CSB has already completed two (2) of the recommendations and will be working aggressively to complete the balance within the next six (6) months.

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,

Rafael Moure-Eraso, Ph.D.
Chairperson & CEO

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 March 30, 2015: Update GSS SSP
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 March 30, 2015: Finalize RMF policy and procedure
2014-03	Perform an annual review of all CSB information SSPs and document the review.	By March 30, 2015: Implement RMF policy and procedure
2014-04	Develop and implement a risk management framework for continuous monitoring of CSB information systems.	By March 30, 2015: Implement RMF policy and procedure
2014-05	Create a visitor access record for the server room or document the acceptance of the risk in the GSS SSP.	Completed. Created and posted visitor log in server room
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 March 30, 2015: Finalize RMF policy and procedure
2014-07	Develop and implement a strategy to be able to conduct an orderly shutdown of CSB servers in the event of a power outage when IT personnel are not present.	By June 1, 2015: Develop and implement automated emergency shutdown procedures for servers
2014-08	Create plans of action and milestones for when CSB would either update or replace all systems with known vulnerabilities.	By June 1, 2015: Add POA&M items to update or replace any system with a known vulnerability
2014-09	Update the GSS SSP and have the authorizing official formally accept the risks of operating systems with known vulnerabilities when the organization made a risk-based decision to accept the risks.	By March 30, 2015: Update GSS SSP
2014-10	Update the organization's vulnerability testing methodology to test all devices connected to the network. This should include all printers and multifunctioning devices.	Completed. Include all network devices in the vulnerability scans
2014-11	Implement processes where employees are not performing incompatible property accountability duties.	By June 1, 2015: Update inventory policies and procedures

2014-12	Implement compensating controls to mitigate the risks for having one employee responsible for entering, altering and deleting information within the CSB inventory system without detection, if segregating the property accountability duties are not possible.	By June 1, 2015: Update inventory policies and procedures
2014-13	Develop and implement policies and procedures for safeguarding inventory from waste, loss, unauthorized use, or misappropriation	By June 1, 2015: Update inventory policies and procedures
2014-14	Conduct a review of all items recorded as lost within the CSB inventory system and make a determination regarding the status of the items.	By June 1, 2015: Conduct review of lost items and document final determination of these items
2014-15	Initiate actions to recover the costs for lost items if CSB determines the item was lost due to employee negligence.	By June 1, 2015: Update inventory policies and procedures
2014-16	Update the CSB inventory system with a description for the items designated as lost.	By June 1, 2015: Update inventory database
2014-17	Make a determination whether lost items should be removed from the CSB inventory system.	By June 1, 2015: Conduct review of lost items and document final determination of these items

Distribution

Chairperson and Chief Executive Officer, 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

Managing Director, U.S. Chemical Safety and Hazard Investigation Board

Deputy Managing Director for Administration, U.S. Chemical Safety and Hazard
Investigation Board

Director of Administration, U.S. Chemical Safety and Hazard Investigation Board

Deputy Director of Administration, U.S. Chemical Safety and Hazard Investigation Board