U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2012)

Report No. 13-P-0307 **June 28, 2013**

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

Abbreviations

CIS	Center for Internet Security
CSB	U.S. Chemical Safety and Hazard Investigation Board
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PP&E	Property, Plant, and Equipment
SP	Special Publication
STIG	Security Technical Implementation Guide
USB	Universal Serial Bus

Hotline

To report fraud, waste, or abuse, contact us through one of the following methods:

email: OIG_Hotline@epa.gov
phone: 1-888-546-8740
fax: 202-566-2599
online: http://www.epa.gov/oig/hotline.htm

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW
Mailcode 2431T
Washington, DC 20460

U.S. Environmental Protection Agency
Office of Inspector General

13-P-0307
June 28, 2013

At a Glance

Why We Did This Review

This review was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the Federal Information Security Management Act of 2002.

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. An annual independent evaluation of the program must be performed by the inspector general or an independent external auditor, who shall report the results to the Office of Management and Budget. The U.S. Environmental Protection Agency, Office of Inspector General, which also serves as the Inspector General for the CSB, contracted with KPMG LLP to perform this fiscal year 2012 evaluation.

This report addresses the following CSB goal:

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

For further information, contact our Office of Congressional and Public Affairs at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2013/20130628-13-P-0307.pdf

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2012)

What KPMG Found

KPMG noted that the CSB has an information security program in place that appears to be functioning as designed. KPMG also noted that the CSB takes information security weaknesses seriously, as the CSB is performing vulnerability assessments on its network devices and security configuration assessments on a subset of its network devices. However, KPMG identified areas in which the CSB could improve upon its vulnerability scanning, patch and configuration management, device encryption, scanning software configuration, and inventory of IT assets.

In addition to reviewing the CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. As a result of this assessment, KPMG found un-patched network devices and mobile devices that were not encrypted, which elevated the CSB's risk of system and data compromise by unauthorized users. KPMG also identified that the scanning tool used by the CSB for providing visibility into its network devices was not providing adequate visibility for its IT devices included within its physical inventory. KPMG also identified 130 personal computers for a staff of 44 members, six decommissioned Blackberries, two decommissioned servers, and 57 obsolete assets identified in the prior year audit that were not retired, which could allow for misuse or loss of IT devices or data.

KPMG is responsible for the content of the final audit report. The OIG performed the procedures necessary to obtain reasonable assurance about KPMG's independence, objectivity, qualifications, technical approach and audit results.

Recommendations and CSB Corrective Actions

KPMG recommends that the CSB take several actions to remediate the identified weaknesses. These include:

- Patching network devices and implementing baseline configurations.
- Implementing encryption on mobile assets and completing plans to implement tools for continuous monitoring of network devices.

The CSB agreed with the report's findings and recommendations. The CSB asserted that it was in the process of implementing the baseline configurations during the audit and will have the baseline configurations implemented by September 30, 2013. The CSB provided agreed-upon corrective actions for all the recommendations.

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

THE INSPECTOR GENERAL

June 28, 2013

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, D.C. 20037-1809

Dear Dr. Moure-Eraso:

This is a final report on the *Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2012)*, conducted by KPMG LLP on behalf of the Office of Inspector General of the U.S. Environmental Protection Agency. The audit was required to be conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. KPMG is responsible for the final audit report and the conclusions expressed in that report. The OIG performed the procedures necessary to obtain a reasonable assurance about KPMG's independence, objectivity, qualifications, technical approach and audit results in order to accept the conclusions and recommendations.

If you or your staff have any questions regarding the enclosed report, please contact Richard Eyermann, acting assistant inspector general for the Office of Audit, at (202) 566-0565 or eyermann.richard@epa.gov; or Rudolph M. Brevard, director, at (202) 566-0893 or brevard.rudy@epa.gov.

Sincerely,

Arthur A. Elkins

Arthur A. Elkins Jr.

June 28, 2013

SUBJECT: Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2012)

THRU: Arthur A. Elkins Jr.
Inspector General
U.S. Environmental Protection Agency
Office of Inspector General

TO: The Honorable Rafael Moure-Eraso, Ph.D.
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board

Attached is the KPMG LLP final evaluation report on the above subject audit. KPMG LLP performed the Federal Information Security Management Act evaluation on behalf of the U.S. Environmental Protection Agency, Office of Inspector General. This report includes the test results for selected minimally required information security controls defined by the National Institute of Standards and Technology.

If you or your staff have any questions regarding the enclosed report, please contact Richard Eyermann, acting assistant inspector general for the Office of Audit, at (202) 566-0565 or eyermann.richard@epa.gov; or Rudolph M. Brevard, director, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Purpose 1

Background 1

Scope and Methodology 2

Findings 2

Patch and Configuration Management Need Improvement 2
Management of Encryption of USB-Connected Digital Media and Mobile Computing Devices with Information Storage Capability Needs Improvement 4
Scanning Application Needs to Be Updated and Configured to Provide Continuous Monitoring of Network Devices and Operating System Visibility... 5
Management of Unused Information Technology Assets Needs Improvement 6

Recommendations 7

CSB Response and KPMG Comments 7

Status of Recommendations and Potential Monetary Benefits 8

Appendices

A **Microagency FISMA Reporting Template** 9

B **CSB Response to Draft Report** 14

Purpose

The U.S. Environmental Protection Agency, Office of Inspector General, initiated this evaluation 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 (FY) 2012. The U.S. Environmental Protection Agency's Office of Inspector General also serves as the Inspector General for the CSB.

Background

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). 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 agency-wide 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 (IGs) 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 (FIPS) and Special Publication (SP) 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, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and 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 IG or an independent external auditor as determined by the IG.

CSB management is 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 the CSB's information technology (IT) environment.

Scope and Methodology

The scope of our testing included the CSB Information Technology System, the only CSB IT system subject to FISMA reporting requirements.

We conducted our testing by making inquiries of CSB personnel, inspecting relevant documentation, and performing limited technical security testing. Some examples of our inquiries of agency management and personnel included, but were not limited to, the process for documenting audit log reviews and vulnerability scanning. We inspected the training sign-off sheets for key CSB staff, IT inventory listings, and the CSB-published information security policies and procedures.

We performed this evaluation in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted the evaluation from September through November 2012.

Findings

During our evaluation for FY 2012, we noted that the CSB has an information security program in place that appears to be functioning as designed. We also noted that the CSB takes information security weaknesses seriously, as CSB is performing vulnerability assessments on its network devices and security configuration assessments on a subset of its network devices on a regular basis. CSB has also taken steps to greatly reduce the number of excess IT devices by recycling or transferring them to other government agencies. However, during this year’s assessment, we identified areas in which the CSB could improve its vulnerability scanning, patch and configuration management process, encryption of mobile devices including USB-connected devices such as removable hard drives, automated scanning tool configuration, and IT inventory.

Patch and Configuration Management Need Improvement

We performed a security assessment of key CSB system and network devices. During this assessment, we identified vulnerabilities related to un-patched devices. We noted that the CSB has established procedures for performing vulnerability scans of its network devices and remediating the results on a regular basis. The CSB needs to remain vigilant in this area to ensure that vulnerabilities are identified and remediated in a timely manner. We have provided the details to CSB management separately and the CSB has taken actions to mitigate these vulnerabilities by implementing our recommendations or plan to take action after performing some additional research. We also performed a configuration scan using both the Center for Internet Security (CIS) benchmarks as well as Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). We noted that the CSB has improved its management of system configurations by performing configuration assessments on a subset of its network devices using DISA STIGs. However, the CSB did not fully implement the standard baseline configurations to which each of CSB's network devices are required to adhere.

FISMA requires that federal agencies maintain information systems used or operated by the agency, or by a contractor of an agency or other organization on behalf of an agency, in accordance with information security guidance issued by NIST.

NIST SP 800-40 Version 2.0, *Procedures for Handling Security Patches* states that "timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems."

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*, states:

> Control AC-6 Least Privilege – The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
>
> Control CM-2 Baseline Configuration – The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
>
> Control CM-7 Least Functionality, Supplemental Guidance – Organizations consider disabling unused or unnecessary physical and logical ports and protocols.

CSB Board Order 034, *Information Technology Security Program*, states that:

> Recognizing the systematic implementation of up-to-date system patches and security updates is critical to the security of CSB information systems and technology, it is the policy of the Board that such systems and technology shall be maintained with current system patches .and security updates. Such patches and updates shall be loaded on a regular basis using a coordinated process, as described in this Appendix.

These system vulnerabilities were caused by the CSB not having fully implemented standard configuration baselines for its network devices and not consistently following their policy, procedures, or NIST. Un-patched devices significantly elevate the CSB's risk of system and data compromise by unauthorized users, which could lead to the alteration or deletion of critical data and a degradation of system performance. Further, by not having fully implemented standard configuration baselines for all of its network devices and not consistently adhering to the current standard configuration baselines being used for testing configuration settings on the subset of network devices tested, the risk is increased that the system could be exposed to malicious technical attacks or unauthorized/unintentional changes.

Management of Encryption of USB-Connected Digital Media and Mobile Computing Devices with Information Storage Capability Needs Improvement

During our review of the inventory of connected IT assets for the CSB, we identified 3 Apple laptops and 2 external hard drives that were not adequately encrypted.

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems,* states in control MP-4 Media Storage:

The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*];
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

In OMB M-06-16, *Protection of Sensitive Agency Information,* the OMB Deputy Director for Management states:

> The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:
>
> > *Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing.*

The CSB stated that they were in the process of procuring FIPS-compliant encryption software for the Apple laptops and that the external hard drives were not allowed out of the office. Failure to appropriately encrypt USB-connected storage media or mobile computing devices with information storage capability increases the risk of disclosure of non-public and sensitive CSB information.

Scanning Application Needs to Be Updated and Configured to Provide Continuous Monitoring of Network Devices and Operating System Visibility

During our review of the scanning tool used by the CSB to provide an automated capability for visibility into IT assets connected to the CSB network, we determined that the CSB was not able to provide visibility for four classes of IT assets identified in the 2012 CSB physical inventory or track the operating system for each of the devices.

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*, states:

> Control CM-2, Baseline Configuration, Enhancement Supplemental Guidance – Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for unauthorized software to validate organization defined lists of authorized and unauthorized software programs.
>
> Control CM-8, Information System Component Inventory – The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

FISMA Reporting Metrics for Micro Agencies states that:

> The Federal Continuous Monitoring Working Group has determined that Asset Management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices (both authorized/managed and unauthorized/unmanaged) before they can manage the devices for configuration, vulnerabilities, and reachability.

The version of the tool used by CSB during FY 2012 did not allow the CSB to track asset operating systems or continuously monitor network devices. The CSB stated that they were eligible for, and in the process of, implementing an upgrade of the scanning tool that will provide the necessary visibility for all IT assets on the network and the ability to configure the scanning application to continuously monitor for vulnerability weaknesses associated with the CSB's network assets. The CSB indicated that this upgrade would take place in FY 2013. Subsequent to our fieldwork, the CSB informed KPMG on November 7, 2012, they had completed the upgrade of the scanning tool which would mitigate the issue that was identified during fieldwork for FY 2012. Since the upgrade occurred in the following fiscal year (2013), we did not perform any additional testing to validate that the CSB has implemented the current version of the scanning tool or that the new capabilities are operating effectively.

Failure to effectively deploy network scanning applications that can monitor connected devices and their vulnerabilities could lead to unauthorized connections to the network or risk the compromise of non-public and sensitive CSB information.

Management of Unused Information Technology Assets Needs Improvement

During our review of the 2012 Annual CSB Physical Inventory, we noted that CSB has made significant progress in greatly reducing the number of excess IT devices by recycling or transferring them to other government agencies. We found that the CSB had reduced its obsolete inventory by using these means to dispose of 343 of the 400 obsolete inventory items we found in our FY 2011 review. However, continued vigilance is still needed to ensure that progress continues to be made in this area. In FY 2012, in addition to the 57 obsolete devices remaining that were identified in the prior year, we also identified 130 personal computers (desktops and laptops) in inventory for a staff of 44 members, six decommissioned Blackberries, and two decommissioned servers, that were not retired out of 287 total IT devices (e.g., Blackberries and other smartphones, desktops, laptops, netbooks, tablets, USB-connected devices, firewalls, switches, routers, servers).

Statement of Federal Financial Accounting Standards 6, Accounting for Property, Plant, and Equipment (PP&E), states:

> General PP&E shall be removed from general PP&E accounts along with associated accumulated depreciation/amortization, if prior to disposal, retirement or removal from service, it no longer provides service in the operations of the entity. This could be either because it has suffered damage, becomes obsolete in advance of expectations, or is identified as excess. It shall be recorded in an appropriate asset account at its expected net realizable value. Any difference in the book value of the PP&E and its expected net realizable value shall be recognized as a gain or a loss in the period of adjustment. The expected net realizable value shall be adjusted at the end of each accounting period and any further adjustments in value recognized as a gain or a loss. However, no additional depreciation/

> amortization shall be taken once such assets are removed from general PP&E in anticipation of disposal, retirement, or removal from service.

The CSB stated that staff members have requested multiple computer and mobile devices to meet their needs, but did not document these justifications. Also, the CSB has not had the resources or time to complete the activity of removing the excess IT assets. Maintaining an inventory that contains a large number of excess items can allow for the misuse or loss of devices if they are not accounted for. Also, if the devices contain non-public and sensitive information that was not degaussed and lost, this could lead to disclosure of non-public and sensitive CSB information.

Recommendations

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

1. Review and implement patches as required for the network devices.

2. Implement standard baseline configurations for all network devices.

3. Develop and implement a protocol to encrypt, with FIPS-compliant encryption, all mobile devices with information storage capability and USB-connected digital storage media, including Apple assets and USB-connected removable hard drives.

4. Proceed with CSB’s FY 2013 plans to implement the upgraded version of the scanning tool used to track operating systems and continuously monitor network devices.

5. Review the information technology inventory and remove the excess inventory items through the General Services Administration.

6. Document management decisions for assigning multiple computers and mobile devices to staff members.

CSB Response and KPMG Comments

The CSB concurred with the report’s findings and recommendations and provided planned actions to address each recommendation. We modified the finding on baseline configurations to state that the CSB had not fully implemented them. While the CSB had outlined its baseline configurations within its information technology standard operating procedures for a subset of its network devices, the CSB had yet to fully implement baseline configurations for all of its network devices. The CSB plans to implement the baseline configurations by September 30, 2013. The CSB’s complete response is in Appendix B.

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	7	Review and implement patches as required for the network devices.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	Ongoing		
2	7	Implement standard baseline configurations for all network devices.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	9/30/13		
3	7	Develop and implement a protocol to encrypt, with FIPS-compliant encryption, all mobile devices with information storage capability and USB-connected digital storage media, including Apple assets and USB-connected removable hard drives.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	7/31/13		
4	7	Proceed with CSB's FY 2013 plans to implement the upgraded version of the scanning tool used to track operating systems and continuously monitor network devices.	C	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	11/7/12		
5	7	Review the information technology inventory and remove the excess inventory items through the General Services Administration.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	9/30/13		
6	7	Document management decisions for assigning multiple computers and mobile devices to staff members.	O	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	9/30/13		

[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

Microagency FISMA Reporting Template

This appendix contains a printout of the information security data that the CSB submitted to OMB in response to the annual FISMA reporting instructions. The following data were obtained from OMB's CyberScope system.

1. System Inventory

1.1 For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low) in this question, provide the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below. (Organizations with below 5000 users may report as one unit.)

	1.1A Organization Operated Systems			**1.1b Contractor Operated Systems**			**1.1c Systems (from 1.1a and 1.1b) with Security ATO**		
FIPS 199 Category	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**
CSB	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**

1.2 For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Organization operational, information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below.

	1.2a Systems utilizing cloud computing resources		**1.2b Systems utilizing cloud computing resources (1.2a) with a Security Assessment and Authorization**		**1.2c Systems in 1.2a utilizing a FedRAMP authorized Cloud Service Provider**	
FIPS 199 Category	**M**	**L**	**M**	**L**	**M**	**L**
CSB	**0**	**0**	**0**	**0**	**0**	**0**

2. Asset Management

2.0 Provide the total number of organization hardware assets connected to the organization's unclassified network	**279**
2.1 Provide the number of assets in 2.0, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	**198**
2.2 Software Assets: Can the organization track the installed operating system Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0.	Yes (6)

2.2a Can the organization track (for each installed operating system Vendor, Product, Version, and patch- level combination in 2.4) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning?	No As of FY 2013, CSB made network updates that allows it to track (for each installed operating system Vendor, Version, and patch level combination in 2.2) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning

3. Configuration Management

3.1 For each operating system Vendor, Product, Version, and patch-level combination referenced in 2.2, report the following:	
3.1a Whether an adequately secure configuration baseline has been defined.	Yes (4/6)
3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).	109
3.1c For what percentage of the applicable hardware assets (per question 2.0), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1a and provide visibility at the organization's enterprise level?	39%

4. Vulnerability Management

4. Provide the number of hardware assets identified in section 2.0 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.	**185**

5. Identity and Access Management

5.1 Provide the number of Organization unprivileged network user accounts? (Exclude privileged network user accounts and non-user accounts)	**50**	
5.2 How many unprivileged network user accounts are configured to:	5.2a. Require the form of identification listed on the left?	5.2b. Allow, but not require, the form of identification listed on the left?
5.2a (1) (2) User-ID and Password	**50**	**0**
5.2b (1) (2) Two factor-PIV Card	**0**	**0**
5.2c (1) (2) Other two factor authentication	**0**	**0**
5.3 Provide the number of Organization privileged network user accounts (Exclude non-user accounts and unprivileged network user accounts)?	**3**	
5.4 How many privileged network user accounts are configured to:	5.4a. Require the form of identification listed on the left?	5.4b. Allow, but not require, the form of identification listed on the left?
5.4a (1) (2) User-ID and Password	**3**	**0**
5.4b (1) (2) Two factor-PIV Card	**0**	**0**
5.4c (1) (2) Other two factor authentication	**0**	**0**

6. Data Protection

6. Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table.		
Mobile Assets Types (each asset should be recorded ***no more than once*** in each column)	6.a. Estimated number of mobile hardware assets of the types indicated in each row	6.b. Estimated number assets from column a ***with adequate encryption of data on the device.***
6.a(1) / 6.b(1)Laptop Computers, Netbooks, and Tablet-Type Computers	**103**	**100**
6.a(2) / 6.b(2)Personal Digital Assistant	**0**	**0**
6.a(3) / 6.b(3) BlackBerries and Other Smartphones	**42**	**42**
6.a(4) / 6.b(4) USB connected devices (e.g., Flashdrives and Removable Hard Drives)	**52**	**50**
6.a(5) / 6.b(5) Other mobile hardware assets	**0**	**0**

7. Boundary Protection

7. Provide the percentage of external connections passing through a TIC/MTIPS.	**0**

8. Training and Education

8. Provide the number of the Organization’s network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually).	**44**

9. Remote Access / Telework

<table>
<tr><td colspan="6">9.1 Provide the estimated total number of annual remote connections the Organization provides to allow users to connect to near-full access to the Organization’s normal desktop LAN/WAN resources/services.</td><td><b>5,550</b></td></tr>
<tr><td colspan="7">9.1.a For those connections counted above in 9.1, provide the estimated number of those connections that:</td></tr>
<tr><td colspan="2">• REQUIRE the kind (<b><i>and only the kind</i></b>) of authentication indicated in 10.1a columns a-d. (List all other connections by connection method in 10.1a column e)
• For each Type of connection listed below</td><td>9.a-1) ONLY User-ID and Password (KFM)
<b>5,550</b></td><td>9.b-2) ONLY Two factor-PIV Card (AP)
<b>0</b></td><td>9.c-3) ONLY Other two factor authentication
<b>0</b></td><td>9.d-4) ONLY one other method. (Please describe in the
<b>0</b></td><td>9.e-5) Connections that may have been authenticated
<b>0</b></td></tr>
<tr><td rowspan="5"><b>Type of Connection</b></td><td><b>9.a-la/1b/1c/1d/1e</b> Dial-up</td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td></tr>
<tr><td><b>9.a-2a/2b/2c/2d/2e</b> Virtual Private Network (<i>not</i> clientless)</td><td><b>5,550</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td></tr>
<tr><td><b>9.a-3a/3b/3c/3d/3e</b> Virtual Private Network (clientless) including SSL, TLS, etc.</td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td></tr>
<tr><td><b>9.a-4a/4b/4c/4d/4e</b> Citrix</td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td></tr>
<tr><td><b>9.a-5a/5b/5c/5d/5e</b> Other</td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td></tr>
</table>

CSB Response to Draft Report

Chemical Safety and
Hazard Investigation Board

2175 K Street, NW • Suite 650 • Washington, DC 20037-1809
Phone: (202) 261-7600 • Fax: (202) 261-7650
www.csb.gov

Rafael Moure-Eraso, Ph.D.
Chairperson

May 29, 2013

Melissa Heist
Assistant Inspector General for Audit
U.S. Environmental Protection Agency
Office of Inspector General
1200 Pennsylvania Ave
Washington, DC 20460

Dear Ms. Heist:

We have reviewed your draft report on the independent evaluation of the Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Management Act (FISMA).

As reported, the CSB takes information security weaknesses seriously and works diligently each year to address the recommendations from the FISMA audits. Consequently, the agency made significant progress in completing actions on FISMA findings from prior years. For instance, in response to the OIG's recommendation FY11-OIG-IT-02 on removing excess IT equipment inventory, the CSB launched an initiative that successfully deinventoried 343 of 400 obsolete IT equipment items. This represents over 85 percent of the items identified during the FY 2011 FISMA audit and was a considerable undertaking by my staff.

With regard to the most recent audit, the agency has one clarification to make regarding the audit's finding on baseline configurations. The report states that "the CSB did not document the standard baseline configurations to which each of CSB's network devices are required to adhere." In response to FY 2012 audit request number five, which explored this issue, the CSB provided section eight of its IT Standard Operating Procedure, which was developed pursuant to the FY 2012 FISMA audit recommendation and details the baseline configurations for its various operating systems. This procedure outlines the baseline configuration for the CSB devices. We would therefore request that the language be clarified to state that the CSB has not yet fully implemented the standard baseline configurations. Our intention is to complete this by the end of the fiscal year.

With the exception of this finding on baseline configurations, the CSB agrees with the FY 2012 findings and recommendations of your draft report. Attached is a table with our planned actions to address each finding and targeted completion dates. Please contact Allen Smith at 202-261-7638, or Charlie Bryant at 202-261-7666 for further information on any of these items.

Sincerely,

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

Enclosure

FY 2012 FISMA Recommendation	Completed or Planned Actions
1. Review and implement patches as required for the network devices.	Ongoing The CSB installed or completed the installation of the missing patches identified in the scan and will continue to actively review and patch network devices.
2. Develop and implement standard baseline configurations for all network devices.	By September 30, 2013, the CSB will: Implement its standard baseline configuration as documented in section eight its SOP.
3. Develop and implement a protocol to encrypt, with FIPS compliant encryption, all mobile devices with information storage capability and USB connected digital storage media, including Apple assets and USB connected removable hard drives.	By July 31, 2013, the CSB will: Encrypt the identified Apple and network storage devices using FIPS 140-2 validated encryption software.
4. Proceed with CSB's FY 2013 plans to implement the upgraded version of the scanning tool used to track operating systems and continuously monitor network devices.	Completed.
5. Review the information technology inventory and remove the excess inventory items through the General Services Administration.	By September 30, 2013, the CSB will: Continue the de-inventory program to remove the remaining obsolete items from the IT inventory.
6. Document management decisions for assigning multiple computers and mobile devices to staff members.	By September 30, 2013, the CSB will: Document the justifications for additional IT computing devices.