U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

The U.S. Chemical Safety and Hazard Investigation Board Complies With the Federal Information Security Management Act (Fiscal Year 2013)

Report No. 14-P-0181 **April 10, 2014**

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
FDCC	Federal Desktop Computer Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
GSS	General Support System
IG	Inspector General
IT	Information Technology
LAN/WAN	Local Area Network/Wide Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
SP	Special Publication
STIG	Security Technical Implementation Guide
TIC/MTIPS	Trusted Internet Connections/Managed Trusted Internet Protocol Services
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: 1-202-566-2599
online: http://www.epa.gov/oig/hotline.htm

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

Suggestions for Audits or Evaluations

To make suggestions for audits or evaluations, contact us through one of the following methods:

email: OIG_WEBCOMMENTS@epa.gov
phone: 1-202-566-2391
fax: 1-202-566-2599
online: http://www.epa.gov/oig/contact.html#Full_Info

write: EPA Inspector General
1200 Pennsylvania Avenue, NW
Mailcode 2410T
Washington, DC 20460

U.S. Environmental Protection Agency
Office of Inspector General

14-P-0181
April 10, 2014

At a Glance

Why We Did This Review

This evaluation was performed 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. 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's Office of Inspector General, which also serves as the Inspector General for the CSB, contracted with KPMG LLP to perform this fiscal year 2013 evaluation.

This report addresses the following CSB goal:

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

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20140410-14-P-0181.pdf

The U.S. Chemical Safety and Hazard Investigation Board Complies With the Federal Information Security Management Act (Fiscal Year 2013)

What KPMG Found

KPMG determined that the CSB has an information security program in place that appears to be functioning as designed. The CSB takes information security weaknesses seriously and is performing vulnerability assessments on its network devices and security configuration assessments on a subset of its network devices.

The CSB has an information security program in place that is functioning as designed; the CSB takes information security weaknesses seriously.

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

KPMG made no recommendations during this evaluation cycle. Evaluation work during this period disclosed that the CSB has taken sufficient actions to close all open recommendations noted during the fiscal year 2012 audit.

The CSB concurred with all report findings.

Noteworthy Achievements

During fiscal year 2013, the CSB implemented patching policy and procedures for its core network devices and computers. This included defining the associated baselines for these devices. The CSB also implemented the current version of its network security and patch management software, which allows greater insight into devices connected to the CSB general support system.

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

THE INSPECTOR

April 10, 2014

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, *The U.S. Chemical Safety and Hazard Investigation Board Complies With the Federal Information Security Management Act (Fiscal Year 2013),* conducted by KPMG LLP on behalf of the Office of Inspector General of the U.S. Environmental Protection Agency. The evaluation 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 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 results in order to accept the conclusions.

If you or your staff have any questions regarding the enclosed report, please contact Kevin Christensen, acting Assistant Inspector General for Audit, at (202) 566-1007 or christensen.kevin@epa.gov; or Rudolph M. Brevard, Director, at (202) 566-0893 or brevard.rudy@epa.gov.

Sincerely,

Arthur A. Elkins Jr.

April 10, 2014

SUBJECT: The U.S. Chemical Safety and Hazard Investigation Board Complies With the Federal Information Security Management Act (Fiscal Year 2013)

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 Kevin Christensen, acting Assistant Inspector General for Audit, at (202) 566-1007 or christensen.kevin@epa.gov; or Rudolph M. Brevard, Director, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Appendices

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) 2013. The U.S. Environmental Protection Agency's Office of Inspector General also serves as the Inspector General for the CSB.

Background

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

KPMG LLP was contracted to perform the Federal Information Security Management Act evaluation on behalf of the U.S. Environmental Protection Agency, Office of Inspector General. 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 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 2013.

Summary of Results

During our evaluation for FY 2013, we did not identify any issues related to CSB's information security management program. Additionally, CSB also took sufficient action to close out all prior recommendations noted during the fiscal year 2012 audit. The following is a summary of the results from the procedures we performed to respond to the OMB Micro Agency Questions which we have included Appendix A.

CSB has a single general support system (GSS) with an impact level of moderate which is authorized to operate. CSB has 293 information technology assets that are connected to the GSS or used by the CSB staff to perform their assigned duties. The information technology assets include desk tops, laptops, flash drives, network devices, servers, smart phones, and tablets.

Currently 66.9% of the information technology assets have an automated capability to provide asset information at an enterprise level. CSB accomplished this by configuring commercial off-the-shelf network security and patch management, and mobile device management software for its laptops, desktops, smart phones, and tablets. The network security and patch management software has also been configured to prevent unauthorized software from being installed on CSB laptops, desktops, and servers. To track operating system and patch levels, CSB uses its network security management software to scan laptops, desktops, and servers on a bi-weekly basis. CSB uses its mobile device management software to scan smart phones and tablets.

CSB is using six different operating systems in their environment. For the operating systems that are present in CSB's environment, they follow approved baselines recommended by the National Institute of Standards and Technology (NIST) which include FDCC and DISA STIGS. CSB has configured 180 of their devices to automatically report vulnerability information at the enterprise level by using its network security and patch management software. CSB also supplements this testing using another NIST-recognized vulnerability application to test its network and connected devices. To control and secure their internet activity from their two locations, all traffic is passed through the TIC/MTIPS.

CSB staff is a mobile work force and they have encrypted mobile devices with FIPS 140-2 validated encryption:

- 85 Laptops
- 9 Tablets
- 40 Smart phones
- 70 USB Devices

The CSB GSS has 78 user accounts which includes standard users, system accounts, privileged accounts. CSB has configured standards and privileged accounts to be accessed by user ID and password. CSB has also enabled remote access for 50 of the user accounts to access CSB GSS resources. The remote access is limited to VPN, SSL Connection, and Smart Phones. Access to these remote access methods are secured with user name and password or a PIN. There are currently 44 full-time employees at CSB and all the individuals have completed their annual security awareness training.

CSB Response and KPMG Comments

The CSB concurred with all report findings. 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
		No recommendations.					

[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

Micro Agency 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.

Section 1: System Inventory				
For each of the FIPS 199 systems' categorized impact levels (H=high, M=moderate, L=low) in this question, what is the total number of information systems by organization.				
Agency	**Impact Level**	**1.1.1 Organization Operated System**	**1.1.2 Contractor Operated System**	**1.1.3 Systems (from 1.1.1 and 1.1.2) with Security ATO**
CSB	High	0	0	0
	Moderate	1	0	1
	Low	0	0	0
	Not Categorized	0	0	0
	Total	1	0	1

Section 2: Asset Management		
2.1	What is the total number of the organization's hardware assets connected to the organization's unclassified network?	293
2.2	What percentage of assets in 2.1 have an automated capability (scan/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets?	66.9%
2.3	For what percentage of applicable assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing, or for what percentage does no such software exist for the device type? This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats.	100%
2.4	Can the organization track the installed operating system's vendor, product, version, and patch level combination (s) in use on the assets in 2.1?	Yes
2.4.1	If yes, report the number of patch-level combinations. We assume one operating system per device. In the comments, report the number of devices that boot with multiple operating systems. Note that virtual machines should be counted as assets.	There are 6 reported.

Section 2: Asset Management		
Section 3: Configuration Management		
3.1	For each operating system vendor, product, version, and patch-level combination referenced in 2.4, report the following:	
3.1.1	Has an adequately secure configuration baseline been defined?	Yes
3.1.2	How many hardware assets (which are covered by this baseline, if it exists) have this software?	69
3.1.3	What percentage of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 have an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level?	Desktops: 41.6 % Servers: 100%

Section 4: Vulnerability Management		
4.1	What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level?	61.4%

Section 5: Identity and Access Management		
5.1	How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.).	46
5.2	What percentage of people with an *unprivileged* network account can log onto the network in each of the following ways.	
5.2.1	Allowed to log on with user ID and password.	100%
5.2.2	Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	0%
5.2.3	Allowed, but not required, to log on with a two-factor PIV card.	0%
5.2.4	Required to log on with a non-PIV form of two-factor authentication.	0%
5.2.5	Required to log on with a two-factor PIV card.	0%
5.2.6	Required to conduct PIV authentication at the user-account level.	0%
5.3	How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)	4
5.4	What percentage of people with a *privileged* network account can log onto the network in each of the following ways?	
5.4.1	Allowed to log on with user ID and password.	100%
5.4.2	Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	0%
5.4.3	Allowed, but not required, to log on with a two-	0%

Section 5: Identity and Access Management		
	factor PIV card.	
5.4.4	Required to log on with a non-PIV form of two-factor authentication.	0%
5.4.5	Required to log on with a two-factor PIV card.	0%
5.4.6	Required to conduct PIV authentication at the user-account level.	0%

Section 6: Data Protection		
Mobile Asset Types (each asset should be recorded no more than once in each column)	Estimated number of mobile hardware assets of the types indicated in each row.	Estimated number assets from column a with encryption of data on the device
Laptop computers and netbooks	85	85
Tablet-type computers	9	9
Blackberries and other smartphones	40	40
Other Cellular devices	0	0
USB connected devices (e.g. flashdrives and removable hard drives)	70	70
Other mobile hardware assets (describe types in comments field)	0	0

Section 7: Boundary Protection		
7.1	What percentage of external network traffic to/from the organization’s networks passes through a TIC/MTIPS?	100%
7.2	What percentage of external network/application interconnections to/from the organization’s networks passes through a TIC/MTIPS?	100%
7.3	What percentage of organization email systems sender verification (anti-spoofing) technologies when sending messages? implement	100%

Section 8: Training and Education		
8.1	What percentage of the organization’s network users have been given and successfully completed cybersecurity awareness training in FY2013 (at least annually)?	100%
8.1.1	What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides adequate security after being granted access?	100%

Section 9: Remote Access

9.1	How many people log onto the organization’s remote access solution(s) to obtain access to the organization’s desktop LAN/WAN resources or services?	50
9.2	For remote access, what percentage of people can log onto the organization’s desktop LAN/WAN resources or services in each of the following ways?	
9.2.1	Allowed to log on with user ID and password.	50
9.2.2	Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	0
9.2.3	Allowed, but not required, to log on with a two-factor PIV card.	0
9.2.4	Required to log on with a non-PIV form of two-factor authentication.	0
9.2.5	Required to log on with a two-factor PIV card.	0
9.2.6	Required to conduct PIV authentication at the user-account level.	0

Appendix B

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

March 6, 2014

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

Dear Mr. Brevard:

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) for fiscal year 2013.

As reported, the CSB takes information security weaknesses seriously and works diligently each year to address the recommendations from the FISMA audits. It is as a result of these efforts that we were able to close all of the FY 12 recommendations.

The CSB agrees with the FY 2013 findings of your draft report and I thank you for your efforts in auditing our program.

Sincerely,

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