U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2011)

Report No. 12-P-0363 **March 21, 2012**

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

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
FISMA	Federal Information Security Management Act of 2002
IG	Inspector General
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

U.S. Environmental Protection Agency
Office of Inspector General

12-P-0363
March 21, 2012

At a Glance

Why We Did This Review

The review 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).

Background

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 CSB, contracted with KPMG LLP to perform the fiscal year 2011 evaluation.

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/2012/20120321-12-P-0363.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2011)

What KPMG Found

KPMG noted that CSB has an information security program in place that appears to be functioning as designed. KPMG also noted that CSB takes information security weaknesses seriously, as three of the four prior-year recommendations were resolved. However, KPMG identified areas in which CSB could improve upon its vulnerability scanning and patch management process, and inventory of information technology assets.

In addition to reviewing CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. This assessment disclosed several challenges CSB faces in securing its main information technology system. KPMG found unpatched network devices, which elevated CSB's risk of system and data compromise by unauthorized users. KPMG provided detailed results of its assessment to CSB officials. KPMG also identified 199 excess information technology devices, of a total of 408, which could allow for misuse or loss of information technology devices or data.

What KPMG Recommends

KPMG recommends that CSB review and implement patches for network devices as required, develop and implement standard baseline configurations for network devices, and review the information technology inventory and remove the excess inventory devices through appropriate means.

CSB agreed with the recommendations and provided agreed-upon corrective actions.

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

THE INSPECTOR GENERAL

March 21, 2012

MEMORANDUM

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigations Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2011)
Report No. 12-P-0363

FROM: Arthur A. Elkins, Jr.
Inspector General

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

This final report on the above subject area summarizes the results of information security work performed by KPMG LLP on behalf of the Office of Inspector General of the U.S. Environmental Protection Agency. This report also includes the U.S. Chemical Safety and Hazard Investigations Board's completed Fiscal Year 2011 Federal Information Security Management Report Template, as prescribed by the Department of Homeland Security.

If you or your staff have questions regarding this report, please contact Patricia H. Hill, Assistant Inspector General for Mission Systems, at (202) 566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard, Director for Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

March 21, 2012

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2011)

THRU: Rudolph Brevard
Director, Information Resources Management Assessments
U.S. Environmental Protection Agency
Office of Inspector General

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

Attached is the KPMG LLP final report on the above subject audit. KPMG LLP performed the Federal Information Security Management Act (FISMA) 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 and the Department of Homeland Security.

If you or your staff have any questions regarding this report, please contact Patricia H. Hill, Assistant Inspector General for Mission Systems, at (202) 566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard 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 2011. The U.S. Environmental Protection Agency's Office of Inspector General also serves as the Inspector General for 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 Office of Management and Budget (OMB) and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) 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, 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 realizable/potentially realizable impacts 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 information technology environment. Conditions may exist that mitigate the risk of an identified deficiency, but they were not identified during our testing.

Scope and Methodology

The scope of our testing included the CSB Information Technology System, the only CSB information technology 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 and 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 2011.

Findings

During our evaluation for fiscal year 2011, we noted that CSB has an information security program in place that appears to be functioning as designed. We also noted that CSB takes information security weaknesses seriously, as CSB has addressed three of the four recommendations made in our report for fiscal year 2010. However, during this year's assessment, we identified areas in which CSB could improve its vulnerability scanning and patch management process, and inventory of information technology assets.

Vulnerability Scanning

Our security assessment of key CSB system and network devices disclosed vulnerabilities related to unpatched devices. We have provided the details to CSB management separately. While CBS Board Order 034 provides policies and procedures for maintaining device security, and CSB drafted and implemented additional supplemental standard operating procedures, CSB personnel did not always follow this guidance to ensure that network devices were appropriately secured. Unpatched devices significantly elevate 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.

Large Number of Unused Information Technology Assets

Our review of the information technology asset listing identified 199 excess devices out of 408 total devices (e.g., Blackberries, laptops, servers). CSB stated that they have not had the resources or time to undertake the activity of removing the excess information technology 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 Chairman, U.S. Chemical Safety and Hazard Investigation Board:

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

2. Develop and implement standard baseline configurations for the network devices.

3. Review the information technology inventory and remove the excess inventory items by using the appropriate means through the General Services Administration.

CSB Response and KPMG Comments

CSB concurred with the report findings and recommendations, and provided planned actions to address each finding and milestones for completion. KPMG considers all recommendations open and will review CSB's actions during the fiscal year 2012 audit.

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	3	Review and implement patches as required for the network devices.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	Ongoing		
2	3	Develop and implement standard baseline configurations for the network devices.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	07/31/12		
3	3	Review the information technology inventory and remove the excess inventory items by using the appropriate means through the General Services Administration.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	09/30/12		

[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

Microagency FISMA Reporting Template

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

Micro Agency Report

Section Report

2011

Annual FISMA Report

Chemical Safety Board

Section 1: System Inventory

1. For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Agency operational, FISMA reportable, systems by Agency component (i.e. Bureau or Sub-Department Operating Element).

Agency/ Component		1a. Agency Operated Systems	1b. Contractor Operated Systems on Behalf of the Agency.	Total Systems	1c. Number of systems in 1a. and 1b. combined with security authorization to operate.	1d. Systems or Services leveraging a public cloud.	1e. Number of Systems and Services in 1d. with a Security Assessment and Authorization to utilize.
CSB	High	0	0	0	0	0	0
	Moderate	1	0	1	1	0	0
	Low	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0
	Sub-Total	*1*	*0*	*1*	*1*	0	0
Agency Totals	High	0	0	0	0	0	0
	Moderate	1	0	1	1	0	0
	Low	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0
	Sub-Total	*1*	*0*	*1*	*1*	0	0

Section 2: Asset Management

2. Provide the total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, blackberry, etc.). (Responses to this question will be used as a denominator in calculating agency benchmarks as a percentage)

408

2a. Provide the number of Agency information technology assets, connected to the network, (e.g. router, server, workstation, laptop, etc.) where an automated capability provides visibility at the Agency level into asset inventory information.

209

Section 3: Vulnerability Management

3. Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (e.g. Common Vulnerabilities and Exposures - CVE).

99

Section 4: Identity and Access Management

4. Provide a working URL to the Agency's progress update for HSPD-12 implementation.

http://www.csb.gov/UserFiles/file/HSPD-12%20Reporting%20Template%20and%20Instructions%20updated%2009012011.pdf

5. What is the number of Agency network user accounts? (Exclude system and application accounts utilized by processes)

51

6. How many network user accounts are configured to require PIV to authenticate to the Agency network(s)?

0

Section 5: Data Protection

7. Provide the total number of:

7.1. Mobile computers and devices (excluding laptops)

7.1(a). Netbooks

4

7.1(b). Tablet-type computers

2

7.1(c). Blackberries

117

7.1(d). Smartphones

0

7.1(e). USB devices (Flash drives and external hard drives)

52

7.1(f). Other

0

7.2. Laptops Only

122

7.3. Mobile computers and devices (excluding laptops)

7.3(a). Netbooks

0

7.3(b). Tablet-type computers

0

7.3(c). Blackberries

0

7.3(d). Smartphones

0

Section 5: Data Protection

7.3(e). USB devices (Flash drives and external hard drives)

0

7.3(f). Other

0

7.4. Laptops only

25

Section 6: Boundary Protection

8. Provide the percentage of external connections passing through a TIC/MTIPS. (Applies to all Federal Civilian Agencies. All others should respond N/A.)

0%

Section 7: Training and Education

9. Provide the number of Agency users with network access privileges that have been given security awareness training annually.

55

Section 8: Remote Access and Telework

10. Provide the number of remote access connection methods (e.g. Dial-up, VPN, Clientless-VPN or SSL, etc.) the Agency offers to allow users to connect remotely to full access of normal desktop Agency LAN/WAN resources/services. Connection methords refer to options the Agency offers to users allowing them to connect remotely.

3

CSB Response to Draft Report

Chemical Safety and Hazard Investigation Board

Hon. Rafael Moure-Eraso
Chairperson

Hon. John S. Bresland
Board Member

Hon. Mark Griffon
Board Member

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

March 2, 2012

Rudolph Brevard
Director, Information Resource Management Assessments
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).

As reported, the CSB takes information security weaknesses seriously and made significant progress in completing actions on FISMA findings from prior years. Specifically, the CSB took the necessary steps to close three of four FY 2010 findings. The remaining recommendation, FY10-OIG-IT-02, is on schedule to meet a target completion date of July 31, 2012. This action will also satisfy the requirements to close one of the FY2011 findings, FY11-OIG-IT-02, to develop and implement standard baseline configurations for agency network devices.

We also agree with the FY 2011 findings and recommendations listed on page 3 of your draft report. Attached is table with our planned actions to address each finding and milestones for completion. 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 2011 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 four missing patches identified in the scan and will continue to actively review and patch network devices.
2. Develop and implement standard baseline configurations for the network devices.	**By July 31, 2012, the CSB will:** Develop and implement standard baseline configurations.
3. Review the information technology inventory and remove the excess inventory items by using the appropriate means through the General Services Administration.	**By September 30, 2012, the CSB will:** Reduce excess information technology items inventory by 75%.