U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2010)

Report No. 11-P-0148

March 8, 2011

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

11-P-0148
March 8, 2011

At a Glance

Catalyst for Improving the Environment

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, Office of Inspector General, contracted with KPMG LLP to perform the fiscal year 2010 evaluation.

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

The full report is at:
www.epa.gov/oig/reports/2011/20110308-11-P-0148.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2010)

What KPMG Found

KPMG noted that CSB does have an information security program in place that appears to be functioning as designed. KPMG also noted that CSB does take information security weaknesses seriously, as 8 of the 10 prior-year recommendations were resolved. However, KPMG identified areas in which CSB could improve upon its vulnerability scanning management process.

In addition to reviewing CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. This assessment revealed several challenges CSB faces in securing its main information technology system. KPMG found insecure system protocols, default configuration settings, and unpatched network devices, which significantly elevated CSB's risk of system and data compromise by unauthorized users. KPMG provided detailed results of its assessment to CSB officials, and CSB worked proactively during the testing to address any identified high-risk issues.

What KPMG Recommends

KPMG recommends that CSB perform vulnerability scans and document audit log reviews consistently; implement baseline configurations for network devices; and develop, maintain, and test a contingency plan for the Information Technology System in accordance with National Institute of Standards and Technology guidance.

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

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

THE INSPECTOR GENERAL

March 8, 2011

MEMORANDUM

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigations Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2010)
Report No. 11-P-0148

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 technology security work performed by KPMG LLP under the direction of the U.S. Environmental Protection Agency, Office of Inspector General. The report also includes the U.S. Chemical Safety and Hazard Investigations Board's completed Fiscal Year 2010 Federal Information Security Management Report Template, as prescribed by the Office of Management and Budget.

The estimated cost for performing this audit, which includes contract costs and Office of Inspector General contract management oversight, is $42,026.

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.

January 4, 2011

SUBJECT: Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with Federal Information Security Management Act for Fiscal Year 2010.

THRU: Arthur A. Elkins, Jr.
Inspector General
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.

If you or your staff have any questions regarding this report, please contact Rudolph Brevard at (202) 566-0893 or brevard.rudy@epa.gov; or Gina Ross, Project Manager, at (202) 566-1041 or ross.gina@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 2010.

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 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 2010.

Findings

During our evaluation for fiscal year 2010, we noted that CSB does have an information security program in place that appears to be functioning as designed. We also noted that CSB does take information security weaknesses seriously, as CSB has addressed 8 of the 10 recommendations made in our report for fiscal year 2009. However, during this year's assessment, we identified areas in which CSB could improve its vulnerability scanning management process. We also reissued two of the prior-year recommendations: (1) develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034, *Information Technology Security Program*, and NIST guidance; and (2) continue to document audit log reviews in accordance with CSB's audit log review standard operating procedure.

Vulnerability Scanning

Our security assessment of key CSB system and network devices revealed vulnerabilities related to insecure system protocols, default configurations, and 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. Insecure protocols, default configurations, and 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.

Contingency Plan

CSB does not have a documented and tested contingency plan for the Information Technology System. CSB Board Order 034 documents a policy and procedure for developing and maintaining a system contingency plan. Further, CSB performs some contingency planning activities, including the periodic backup of data and the rotation of backup data to an offsite location. However, a system-specific contingency plan has not been developed or tested. CSB management did not commit the required resources and leadership to develop a contingency plan for the Information Technology System. Without a documented and tested contingency plan completed in accordance with NIST guidance, CSB is at increased risk that it would not be able to recover Information Technology System capabilities should a significant incident occur.

Audit Logs

CSB has developed a procedure for performing and documenting log reviews for the Information Technology System. According to CSB officials, security staff members perform a daily or weekly review of the Information Technology System audit logs. However, CSB did not begin documenting the log reviews until October 2010. The lack of a documented procedure for performing and documenting system audit log reviews increases CSB's risk that the log reviews will not be conducted in a consistent manner, which could lead to increased risk of not detecting key security violations and events.

Recommendations

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

1. Perform vulnerability scans on a regular basis, such as monthly or quarterly.

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

3. Develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.

4. Continue to document audit log reviews in accordance with CSB's audit log review standard operating procedure.

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. In addition, CSB believed that it completed actions to address recommendation 1. KPMG considers all recommendations open and will review CSB's actions during the fiscal year 2011 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	Perform vulnerability scans on a regular basis, such as monthly or quarterly.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	02/01/11*		
2	3	Develop and implement standard baseline configurations for network devices.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	03/30/11		
3	3	Develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	09/30/11		
4	3	Continue to document audit log reviews in accordance with CSB's audit log review standard operating procedure.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board	09/30/11		

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

* The determination to close recommendation 1 will be made in the next audit.

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

2010

Annual FISMA Report

Chemical Safety Board

Section 1: System Inventory

1. For each of the subparts in this question, provide the total number of Agency operational systems (both Agency operated and contractor operated) by Agency component (i.e. Bureau or Major Operating Element).

Agency/ Component		1a. Agency Operated Systems	1b. Contractor Operated Systems	Total Systems	1c. Number of Systems with a Current Authorization to Operate
CSB	High	0	0	0	0
	Moderate	1	0	1	1
	Low	0	0	0	0
	Not Categorized	0	0	0	0
	Sub-Total	***1***	***0***	***1***	***1***
Agency Totals	High	0	0	0	0
	Moderate	1	0	1	1
	Low	0	0	0	0
	Not Categorized	0	0	0	0
	Sub-Total	***1***	***0***	***1***	***1***

Section 2: Asset Management

2. Provide the estimated total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, blackberry, etc.).

356

Comments:

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

188

Comments:

Section 3: Vulnerability Management

3. Provide the estimated number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (e.g. Common Vulnerability Enumerations).

110

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/CSB_HSPD-12.pdf

5. What is the estimated number of Agency network user accounts?

52

Comments:

6. What estimated number of Agency network user accounts are configured to require PIV credentials to authenticate to the Agency network(s)?

0

Section 5: Data Protection

7. Provide the estimated number of:

7a. Portable computers (i.e. laptops).

115

7b. Those portable computers in (a) that have all user data encrypted with FIPS 140-2 validated encryption.

9

Section 6: Boundary Protection

8. Provide the percentage of external connections passing through a TIC/MTIPS.

0% to 0%

Section 7: Training and Education

9. Provide the number of Agency users with log-in privileges that have been given security awareness training annually.

49

Comments:

Section 8: Remote Access and Telework

10. Provide the estimated number of remote access connection methods (connection methods the Agency offers to allow users to connect remotely such as VPN, RSA, etc.) to Agency LAN/WAN resources/services.

3

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

February 1, 2011

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 made significant progress in completing actions on FISMA findings from prior years. Specifically, the CSB took the necessary steps to close eight out of ten FY 2009 findings. The agency has since closed recommendation FY09-OIG-IT-08. The final remaining recommendation, FY09-OIG-IT-05, is on schedule for completion by September 30, 2011.

We also agree with the FY 2010 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

1. Perform vulnerability scans on a regular basis, such as monthly or quarterly.	Completed. **SOP updated to require quarterly vulnerability scans and scans completed in October 2010 and Jan 2011.**
2. Develop and implement standard baseline configurations for network devices.	By March 30, 2011, the CSB will: **Develop and implement baseline network device configurations.**
3. Develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.	By September 30, 2011, the CSB will: **Develop and implement a Contingency Plan for the CSB General Support System (GSS).**
4. Continue to document audit log reviews in accordance with CSB's audit log review standard operating procedure.	By September 30, 2011, the CSB will: **Continue documenting audit log reviews in the GSS following guidance in CSB IT SOP on log management.**