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

SEP 28 2004

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal 2004
Report No. 2004-S-00006

FROM: Patricia H. Hill, Director
Business Systems Audits (2421T)

TO: Carolyn W. Merritt, Chairman
United States Chemical Safety and Hazard
Investigation Board

Attached is the final report entitled *Federal Information Security Management Act: Fiscal 2004 Status of CSB's Computer Security Program.* This report synopsizes the results of information technology security work performed by KPMG LLP on behalf of the U.S. Environmental Protection Agency's Office of Inspector General (OIG). This report includes KPMG's completed FY04 FISMA Reporting Template, as prescribed by the Office of Management and Budget (OMB), as well as detailed results of their evaluation.

In accordance with OMB reporting instructions, I am forwarding this report to you for submission, along with your Agency's required information, to the Director, OMB.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0894 or Rudolph M. Brevard at (202) 566-0893.

Attachment

KPMG LLP
2001 M Street, NW
Washington, DC 20036

September 24, 2004

Mr. Rudy Brevard, Assignment Manager
U.S. Environmental Protection Agency
Office of Inspector General
Mail Code 2421T
1200 Pennsylvania Avenue, NW
Washington, DC 20460

Re: Chemical Safety Board Federal Information Security Management Act (FISMA) Evaluation

Dear Mr. Brevard

Thank you for providing KPMG LLP (KPMG) with the opportunity to assist the U.S. Environmental Protection Agency Office of Inspector General in performing an evaluation of the Chemical Safety Board's compliance with the Federal Information Security Management Act.

Accompanying this transmittal/closure letter are three copies of our final report deliverable. With this transmittal/closure letter, we are representing that we have delivered our final work products to your office under the terms and conditions of our May 18, 2004 proposal. Thus, we have met the requirements of engagement closure.

Please contact Tony Hubbard at 202-533-4324 or Rebecca Mann at 804-782-4276 if you have any questions or comments. We look forward to continuing to provide services to your office in the future.

KPMG LLP

Executive Summary

Introduction

The Office of the Inspector General (OIG) tasked KPMG LLP (KPMG) to conduct an independent evaluation of the United States Chemical Safety and Hazard Investigation Board's (CSB) information security program and practices. We performed this evaluation pursuant to Title III of the Electronic Government Act, subtitled "The Federal Information Security Management Act (FISMA)" and the Office of Management (OMB) fiscal 2004 FISMA reporting instructions. Our objectives were to evaluate CSB's information security management practices and to determine whether it has taken corrective actions in response to issues identified in its fiscal 2003 FISMA report to OMB.

To perform this evaluation, we requested all documentation related to prior CSB audits, security evaluations, security program reviews, vulnerability assessments, and other reports addressing CSB's information security program and practices. In addition, we reviewed documentation supporting security training, security-related capital planning efforts for technology, memoranda regarding information security policies, and plans for future information security assessments. From the information and interviews with CSB officials, we evaluated CSB's progress in meeting OMB's performance measures specific to agency responsibilities outlined in the Act.

Reporting Requirements

OMB issued reporting guidance to agencies, which Inspectors General must use to report results of IT security reviews. Additionally, agencies must report on remediation activities regarding previously identified issues. In fiscal 2004, OMB established an abridged reporting format for agencies employing less than 100 employees. At the time of our evaluation, CSB employed approximately 45 personnel and was eligible to report its results using OMB's abridged reporting format. However, CSB management requested KPMG review its systems with more detail than required in the revised draft FISMA guidance. As such, this report contains both detailed results of our evaluation, as well as CSB's fiscal 2004 FISMA report in the abridged format.

Results in Brief

CSB has made significant progress in mitigating previously identified security program weaknesses, but officials indicated that a lack of personnel and financial resources contributed to many weaknesses still not being fully addressed. This evaluation disclosed several areas that require management's attention to address four outstanding security weaknesses, as well as one weakness identified during this review. We found CSB had not:

- completed and documented a risk assessment for IT operations and assets. Additionally, technical controls such as file and e-mail encryption had not been implemented;

- developed or established an IT security awareness program to provide training to all personnel;

- documented or formally approved its incident handling procedures;

- conducted a formal certification and accreditation review to ensure implemented managerial, technical, and operational controls are working as intended. Furthermore, senior CSB officials had not issued formal authority for these systems to operate, thereby accepting the risks these systems pose to the agency's assets, operations, and personnel; and

- instituted a formal patch management process to detect, apply, and track system and software updates as they become available

Table of Contents

Appendix

Federal Information Security Management Act
Status of CSB's Computer Security Program

A. System Inventory and IT Security Performance

A.1 The agency Chief Information Officer (CIO) and Inspector General shall identify the total number of agency programs/systems and contractor operations or facilities that were reviewed using NIST 800-26, "Security Self-Assessment Guide for Information Technology Systems," in FY04.

During fiscal 2004, CSB identified three systems, corresponding directly to the following three main programs:

- Investigations
- Recommendations and Technical Product Systems
- Administrative Functions

Each program uses the same IT systems to complete its tasks. However, CSB recognizes the three systems supporting these programs as independent systems. CSB uses commercial-off–the-shelf (COTS) software packages in its IT environment. For example, CSB uses Microsoft Office and Outlook suites for word processing, spreadsheets, databases, and e-mail exchanges.

CSB did not use the NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to re-evaluate their systems and programs for FY 2004. CSB officials indicated a new self-assessment was not warranted due to the agency's small size and because they completed a self-assessment in fiscal 2003.

During fiscal 2004, CSB continued to use the Bureau of Public Debt to process its finances, and the National Business Center to process employee payroll. Periodically, CSB's IT Security Officer (ITSO) reviews these electronic connections to ensure they are secure and meet established encryption standards.

A.2 For each question below, identify the total number of items in each category and identify the total of number which have been reviewed in fiscal 2004.

	Total Number	Percent of Total
a. Number of systems certified and accredited.	0	0%

	Total Number	Percent of Total
b. Number of systems with security control costs integrated into the life cycle of the system.	3	100%
c. Number of systems for which security controls were evaluated in the last year.	0	0%
d. Number of systems with a contingency plan.	3	100%
e. Number of systems for which contingency plan have been tested.	3	100%

None of CSB's systems have been certified or accredited to operate. CSB management does not believe this is a requirement, as none of their systems contain national security information. Nevertheless, we believe that a security certification and accreditation that follows the guidance of NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, allows an entity to meet the Federal requirements outlined in OMB Circular A-130, Appendix III. Such a process would help ensure that CSB implement security controls throughout a system's life cycle in accordance with organizational security policies and Federal guidelines. As such, senior officials would have a stronger basis to accept the risks these systems pose to agency's assets, operations, and personnel.

We reviewed CSB's IT Contingency Plan, which has not changed or been modified since fiscal 2003. The contingency plan covers all three systems, identifies 10 supporting technologies, and the related failsafe methodologies supporting these technologies. CSB has performed periodic tests of the failsafe technologies to ensure that various backup processes would be effective. The contingency plan does not refer to a hot site or alternate processing facilities, but this is appropriate given CSB's small IT environment and reliance on service providers for key processes (i.e., payroll and financial processing).

A.3 Evaluate the degree to which the following statements occur in your agency.

	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	The Chief Operating Officer (COO), in coordination with the IT Manager, has ensured security over contractor operations, based on the security self-assessment conducted in fiscal 2003.
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	No self-assessment conducted for fiscal 2004.
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of NIST.	No review conducted.
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	The inventory database for major IT systems is updated and current.
e. The OIG was included in the development and verification of the agency's major IT system inventory.	The OIG is not included in the verification of the system inventory.
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	During the fiscal 2004 FISMA review, the OIG and COO agreed on the total number of programs and systems.
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	The COO concurs with all major IT investments and gives approval accordingly.
h. The agency has begun to assess systems for e-authentication risk.	No. CSB documented resource requirement in fiscal 2004 IT Capital.
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

B. Identification of Significant Deficiencies

B.1 Identify all significant deficiencies in policies, procedures, or practices as identified and required to be reported under existing law in FY04. Identify the number of significant deficiencies, and the number of significant deficiencies repeated from FY03. For each significant deficiency, indicate whether a Plan of Action and Milestone (POA&M) has been developed for that specific significant deficiency.

CSB has five significant deficiencies in polices, procedures, and practices for fiscal 2004. Four significant deficiencies are reoccurring from fiscal 2003. These include: (1) Implementing essential technical controls such as file and e-mail encryption and completing risk assessments for IT operations and assets; (2) establishing an IT security awareness program to provide training to all personnel; (3) documenting and approving incident-handling procedures; and (4) conducting certification and accreditation reviews of all systems. CSB documented the fifth significant deficiency during fiscal 2004, which was instituting a formal patch management process.

During fiscal 2004, CSB closed one significant deficiency, which was approving its Information Security Plan. We reviewed CSB's Information Security Plan for compliance with security requirements and description of controls specified in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*. Our review determined CSB's Information Security Plan complies with the recommended NIST guidance.

According to CSB officials, the five significant deficiencies are incomplete due to lack of funding. As such, a POA&M was established and documented for each significant deficiency.

C. OIG Assessment of the POA&M Process

C.1 Evaluate the degree to which the following statements reflect the status in your agency

	Evaluation
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Yes
b. Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Yes
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation	Yes

	Evaluation
progress.	
d. CIO develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Yes
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis	Yes
f. The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Yes
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance.	Yes
h. OIG has access to POA&Ms as requested.	Yes
i. OIG findings are incorporated into the POA&M process.	Yes
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	The priority level is not stated on the POA&M.

CSB does not have a Chief Information Officer (CIO). The Chief Operating Officer (COO) currently fills this position. Additionally, CSB appointed an ITSO who is responsible for the development, implementation, and management of the agency-wide security POA&M process. Program officials, in coordination with the COO, develop, implement, and manage POA&Ms for systems they own and operate. Additionally, program officials and the COO report to OMB the status of the POA&Ms on a quarterly basis.

The POA&M is the authoritative agency management tool to identify, monitor, and track agency remedial activities. The POA&M contains a column illustrating the funding requirements for the specific system level POA&M activities. Each item has a designated point of contact, resources required (if applicable), recommendations, milestones, and issue identification date. The POA&M appears to be a comprehensive document addressing weaknesses noted in prior year security reviews. The POA&M contains a scheduled completion date, as well as a status column. The status column indicates whether the milestones were “completed,” “on-going,” or “on-going but on-hold.”

C.2 OIG evaluation of the Certification and Accreditation process.

CSB has not certified and accredited any of its systems to operate. See section A-2 for additional analysis of CSB's certification and accreditation process.

D. Agency-wide Security Configuration Requirements

D.1 Has the CIO implemented agency-wide policies that require detailed, specific security configurations?

The COO established agency-wide policies that require detailed, specific security configurations within the CSB IT environment. Moreover, the CSB Information Security Plan outlines physical security on personal desktops, as well as the use of passwords to gain access to systems.

We conducted a test of CSB's external and internal network infrastructure. Our test indicated CSB has taken reasonable steps to secure its *external* network infrastructure by implementing:

- Border Router protection;
- Fail-over firewall configuration limiting inbound services to only HTTP (web) and SMTP (mail);
- Operating system with security setting configured correctly; and
- Host and network-based Intrusion Detection Systems.

However, our test of CSB's *internal* network infrastructure identified the following vulnerabilities:

- Vendor supplied patches/fixes were not installed in a timely manner;
- Obsolete user accounts remain on the CSB domain; and
- Switches and Printers were configured with no passwords

These internal vulnerabilities, especially the missing patches/fixes, may lead to unauthorized access on the hosts and the compromise of sensitive information

We notified CSB's ITSO of these issues and confirmed that CSB is working to implement an automated patch management system. In addition, the ITSO confirmed the agency would enter stronger passwords on the identified switches and printers.

D.2 Do the configuration requirements implemented above address patching of security vulnerabilities?

CSB has not implemented enterprise monitoring, patching, and tracking software. Currently, CSB updates workstations and servers individually. CSB is using Microsoft's Baseline Analyzer to detect certain Microsoft-related vulnerabilities. However, CSB should implement a stronger system to maximize security assessments. According to CSB management, a lack of financial resource prevents implementation of such a system.

E. Incident Detection and Handling Procedures

E.1 Evaluate the degree to which the following statements reflects the status at your agency:

a. The agency follows documented policies and procedures for reporting incidents internally.

CSB's Information Security Plan policy addresses incident reporting should a security violation occur within the network or physical environment. The policy requires the user to inform the ITSO, as soon as possible, after a security violation has occurred or whenever the user suspects there has been a security violation. CSB is in the process of implementing new security violation reporting procedures. However, these reporting procedures have not been finalized.

b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.

As noted in E.1-A, CSB is in the process of implementing new security violation reporting procedures. However, these reporting procedures have not been finalized.

c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).

As noted in E.1-A, CSB is in the process of implementing new security violation reporting procedures. However, these reporting procedures have not been finalized.

E.2 Incident Detection Capabilities

	Evaluation
a. How many systems underwent vulnerability scans and penetration tests in FY04?	44 workstations and 14 servers
b. What tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?	Web Server Vulnerability Scanners, Enterprise Anti Virus Software, Firewall, Intrusion Detection System (IDS), Host-based IDS, and Network-wide Event Log Manager.

F. Incident Reporting and Analysis

Identify the total number of successful security incidents and identify total number of system affected in FY04.

Category of incident	Total Number of Successful Incidents in FY04	Type of System Affected		
		Systems with complete and up-to-date Certification and Accreditation	Systems without complete and up-to-date Certification and Accreditation	System with known vulnerabilities for which a patch was available
I. Root Compromise	0	0	0	0
II. User Compromise	0	0	0	0
III. Denial of Service Attack	0	0	0	0
IV. Website Defacement	1	0	1	1
V. Detection of Malicious Logic	0	0	0	0
VI. Successful Virus/worm Introduction	0	0	0	0
VII. Other	0	0	0	0

CSB experienced one security incident during fiscal 2004. This incident resulted in CSB's web server being out of production for approximately three hours. The noted security incident affected an unpatched and non-certified and accredited system with known vulnerabilities.

G. Training

G.1 Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?

During fiscal 2004, CSB had not yet implemented a comprehensive security awareness-training program for all employees. The only employee with formal security awareness training is the ITSO. CSB currently does not have a security-training program plan. This is a recurring issue identified in CSB's fiscal 2003 FISMA review, and has been documented as an action item in the POA&M.

Since the fiscal 2003 FISMA review, CSB has implemented some initiatives to conduct security awareness training. CSB has integrated the "Go-Learn" web-based training in order to begin formalized security training for its employees. However, CSB IT security training needs more dedicated resources to implement the program.

CSB officials indicated that a lack of resources has continued to thwart this program's full implementation.

	Evaluation Results
a. Total number of employees in FY04	Approximately 45
b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50.	0
c. Total number of employees with significant IT security responsibilities.	1
d. The Employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-50 and 800-16.	0
e. Briefly describe training provided	Hardware vendor security certification training and Operating System certification training.
f. Total costs for providing IT security training in FY 2004 (in $).	$ 0

G.2 Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?

During fiscal 2004, CSB did not have a formal security awareness training program. As such, CSB did not have agency policies or training procedures regarding peer-to-peer file sharing.

Appendix A

U.S. Chemical Safety and Hazard Investigation Board FY04 FISMA Report

Name of Agency	**U.S. Chemical Hazard and Investigation Safety Board**
Budget for IT security (in thousands)	$ 0
Was a self-assessment using NIST guidelines conducted in FY04? (y/n)	No
Was an independent assessment conducted in FY04? (y/n)	No
If yes, please attach. If no, why was assessment not conducted?	CSB management stated several of the questions were not applicable due to the Agency's relatively small size and since an assessment was performed in 2003. Therefore, in fiscal 2004, CSB did not complete the assessment.
# of significant deficiencies (in policies, procedures, or practices)	5
# of significant deficiencies repeated from last year	4
Total number of systems	3
Number of systems assessed for risk (assessed the risk to operations and assets and determined the level of security appropriate to protect such operations and assets)	0
Number of systems with security plans	3
Number of systems certified and accredited	0
Number of systems with security controls tested FY04	3
Number of systems with contingency plans	3
Number of systems with tested contingency plans	3
Did you report IT security incidents to US-CERT (y/n)	No
How many incidents did you report?	0
Number of employees (including contractors)	45

Name of Agency	U.S. Chemical Hazard and Investigation Safety Board
Number of users receiving IT security awareness training in FY04	0
Number of IT security staff including contractors (employees or contractors with significant IT security responsibilities)	1
Number of IT security staff who received specialized security training in FY04	0
Was an FY04 POA&M submitted to OMB? (y/n)	Yes
Number of weaknesses identified in POA&M	19
Number of weaknesses reported corrected as of 9/24/04	8