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

OFFICE OF
INSPECTOR GENERAL

September 28, 2005

MEMORANDUM

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005
Report No. 2005-2-00030

FROM: Rudolph M. Brevard /s/
Acting Director, Business Systems Audits

TO: The Honorable Carolyn W. Merritt
Chairman and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board

Attached is KPMG's LLP final report on the above subject area. This report synopsizes the results of information technology security work performed by KPMG on behalf of the U.S. Environment Protection Agency's Office of Inspector General (OIG). The report also includes KPMG's completed Fiscal Year 2005 FISMA Reporting Template, as prescribed by the Office of Management and Budget (OMB).

In accordance with OMB reporting instructions, the OIG is 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) 566-0893 or William Coker at (202) 566-2553

Evaluation Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005

September 28, 2005

Abbreviations

C&A	Certification and Accreditation
CIO	Chief Information Officer
CSB	United States Chemical Safety and Hazard Investigation Board
EPA	Environmental Protection Agency
FedCIRC	Federal Computer Incident Response Center
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IATO	Interim Authority to Operate
ITM	Information Technology Manager
ISO	Information Security Officer
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication

September 28, 2005

Mr. Rudolph M. Brevard
Acting Director for Business Systems Audits
U.S. Environmental Protection Agency
Office of Inspector General
Mail Code 2421T
1200 Pennsylvania Avenue, NW
Washington, DC 20460

Re: Transmittal of the Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005.
Contract No: GS-23F-8127H

Dear Mr. Brevard:

Thank you for providing KPMG LLP (KPMG) with the opportunity to assist the U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) in performing the evaluation of the U.S. Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005.

We are pleased to present our final evaluation report for the CSB's compliance with FISMA during Fiscal Year 2005. The delivery of this report concludes our obligations under Purchase Order number 4W-3271-NBLX. Pursuant to the Purchase Order, we will issue our final invoice for this engagement.

We have enjoyed working with you and your staff and look forward to continuing to provide the EPA OIG with quality services. For further information regarding this report, contact the EPA OIG Office of Congressional and Public Liaison at (202) 566-2391.

Very Truly Yours,

KPMG LLP

Table of Contents

Chapters

Appendices

Chapter 1
Executive Summary

Introduction

The Office of Inspector General (OIG) tasked KPMG LLP (KPMG) to assist in performing the FY 2005 Federal Information Security Management Act (FISMA) independent evaluation of the United States Chemical Safety and Hazard Investigation Board's (CSB) information security program and practices. CSB is a small federal entity and as a result, does not have an information security program and related practices comparable to those of larger federal entities; this has been taken into account during the evaluation.

To perform the independent evaluation, we requested 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, documentation supporting security training, security-related information technology (IT) capital planning efforts, memoranda regarding information security policies, and plans for future information security assessments was reviewed. Appendix B of this report lists the documents reviewed as part of this evaluation. Through inspection of the documentation received and inquiry with CSB personnel, we evaluated CSB's progress in meeting Office of Management and Budget's (OMB) FISMA performance measures.

Reporting Requirements

OMB has issued FISMA reporting guidance for "micro-agencies", which OMB defines as an agency with fewer than 100 employees. CSB meets the OMB criteria for a micro-agency and the required reporting template is included at Appendix A. In addition, the EPA OIG requested that KPMG review the CSB information security program in more detail than required for the FISMA micro-agency reporting guidance. Consequently, this report contains additional details on our observations regarding CSB's information security program.

Results in Brief

The CSB IT department underwent significant changes during FY 2005. An Information Technology Manager (ITM), the CSB equivalent to an Information Security Officer (ISO), was appointed in March 2005, filling a vacancy that existed in that position since October 2004. Additionally, during FY 2005, CSB appointed a Chief Information Officer (CIO). Although filling these key security positions were positive steps, the delays in making these appointments hampered CSB's ability to addresses significant

deficiencies noted in the FY 2004 FISMA evaluation, which consequently resulted in the occurrence of these significant deficiencies in the FY 2005 FISMA review.

Under the direction of the CIO and the ITM, CSB hired a contractor to assist the Agency in correcting many of the identified security weaknesses. CSB's aggressive action has resulted in tangible steps to mitigate most of the FY 2005 deficiencies by the end of the calendar year. Below is the status of CSB's significant deficiencies and additional details are in Chapter 2:

- **OIG-IT-01 – Security Certification and Accreditation (C&A)**. Although CSB issued an Interim Authority to Operate (IATO) for its three systems, CSB had not certified or accredited their systems. Additionally, CSB had not categorized its systems in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199, or reviewed the systems using security guidance contained in NIST Special Publications 800-26 and 800-53. CSB officials indicated that the Agency would complete this task by the end of the calendar year after the installation of new servers and the assessment of other identified weaknesses. In addition, CSB indicated that the ITM would complete the required NIST 800-26 self-assessment by end of FY 2005.

- **OIG-IT-02 – Security Control Implementation**. CSB has not addressed prior year security control implementation significant deficiencies. These include the lack of a complete IT risk assessment, lack of technical security controls such as file and e-mail encryption, and lack of an agency-wide software patch management system.

  During the FY 2005 FISMA evaluation, we identified the following additional issues that contribute to CSB's significant deficiency around security control implementation:

  - CSB has not tested its contingency plan within the past year;
  - A documented security configuration policy for CSB networks has not been implemented;
  - E-Authentication risk assessments have not been conducted;
  - Two of the three CSB systems have not had their security controls tested within the past year; and
  - CSB did not perform sufficient oversight for its contractor systems to ensure the systems meet FISMA requirements.

  CSB officials concurred with the findings in this area and took steps to address many of the significant deficiency. CSB obtained contractor support to: (1) review some of the FY 2004 findings and (2) provide recommendations on mitigating the weakness. CSB officials provided action plans to mitigate weaknesses in its Annual Self-Assessment, Risk Assessment, Technical Security Controls, and Patch Management processes by October 2005. CSB also indicated the Agency would update security plans by December 2005. In addition, with the implementation of a new system infrastructure, CSB indicated it would complete the update of its contingency plans by

March 2006. Although CSB provided steps for improving its e-authentication risk assessment and oversight of contractor system process, CSB did not indicated when it would complete these activities.

- **OIG-IT-03 – Security Training.** During FY 2005, CSB implemented a security awareness-training program for its employees, thereby, eliminating a long-standing significant deficiency reported in the FY 2003 and FY 2004 FISMA evaluations. However, CSB's security-awareness training does not include information regarding peer-to-peer file sharing. In response to this finding, CSB indicated it would address this weakness in a separate notification to all staff and update the security-awareness training material.

- **OIG-IT-04 – Security Program Management.** CSB was without a formally appointed ITM from October 2004 through March 2005. During that time, the required FISMA Plan of Action and Milestones (POA&M) was not submitted to OMB. Additionally, CSB had not prioritized the weaknesses identified in the POA&M, which is a key step for addressing the weaknesses. CSB concurred with this finding and indicated the Agency prioritized the weaknesses in its September 2005 POA&M submission to OMB.

- **OIG-IT-05 – Security Incident Handling.** CSB has not approved its incident handling procedures. During FY 2005, CSB developed new procedures for incident handling, but had not approved the procedures. CSB concurred with this finding and indicated it would approve the new procedures by October 31, 2005.

Chapter 2
Results of Independent Evaluation

Objective 1

Evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below.

FIPS 199 Categorization	Total Number of Agency and Contractor Systems	Number Evaluated
Agency Systems		
Not Categorized	2	0
Contractor Systems		
Not Categorized	1	0
Total Systems Not FIPS 199 Categorized	**3**	**0**

CSB has not categorized their three systems according to the FIPS 199[1] criteria, nor has CSB evaluated the systems against NIST Special Publication 800-26[2] or 800-53[3]. To their credit, CSB management has contracted out the tasks needed to complete the FIPS 199 categorization. For FY 2006, CSB plans to consolidate the three systems into one general support system (GSS). **Finding OIG-IT-01**

Objective 2

Identify actual performance in FY 05 by risk impact level and bureau. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

[1] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, sets standards for security categorization of information and information systems through the use of standardized security objectives and ranking criteria.
[2] NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured.
[3] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

Security category	Total Number	Number Reviewed
Total number certified and accredited	0	0
Total number with controls evaluated	1	0
Total number with contingency plan tested	0	0

Although all of CSB's three systems have an IATO, none of the systems have been certified and accredited. The IATO authorization covers a two-year period from September 30, 2004. CSB has obtained contractor support to help address these issues. At the time of our FY 2005 FISMA evaluation, the contractor was in the process of conducting a security control evaluation assessment for the systems, which is a key element of a C&A. **Finding OIG-IT-01**

Additionally, CSB has not evaluated the security controls on two of its three systems nor had CSB tested its contingency plan within the past year. **Finding OIG-IT-02**

Objective 3

Evaluate the agency's oversight of contractor systems, and agency system inventory.

Evaluate the status of the following	Results:
a. The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	No formal evaluations have been conducted on CSB contractor systems or information security controls and processes.
b. The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.	CSB maintains a complete list of all systems, including those operated by contractors. CSB has no national security systems.
c. The OIG generally agrees with the CIO on the number of agency owned systems.	OIG agrees with the CIO's classification of systems and is aware of efforts to consolidate systems into one GSS.
d. The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
e. The agency inventory is maintained and updated at least annually.	Yes.

Evaluate the status of the following	Results:
f. The agency has completed system e-authentication risk assessments.	No E-authentication risk assessments have been conducted.

The CSB ITM currently performs oversight for the Recommendation and Technical Solution System. Contractors administer and maintain this system and report directly to the CSB ITM. However, CSB does not oversee and evaluate the system to ensure compliance with FISMA requirements. **Finding OIG-IT-02**

CSB has consolidated its IT inventory into a Microsoft Access database. Using the database, CSB has the ability to query specific IT equipment. CSB updates the access database at least annually and when any changes/deletions are needed.

CSB has notified the EPA OIG of the number of systems operational at CSB, and the EPA OIG is in agreement with the number of systems. CSB management has proposed to consolidate the three current systems into one GSS and the OIG concurs.

Objective 4

Assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process.

Evaluate the status of the following	Results:
a. The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Yes. The CSB POA&M process appears to be an agency wide process that has incorporated all known IT security weaknesses. The CSB POA&M contains weaknesses, points of contact (POCs), required resources, scheduled completion dates, milestones, milestone changes, how the weakness was identified, and the status of weaknesses.
b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Yes. All IT security weaknesses identified by the program officials are incorporated and managed by the CSB POA&M.
c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Yes. Contractors report weekly and the remaining Program Officials and Contractors report directly to

Evaluate the status of the following	Results:
	CSB security management, who reports to the CIO.
d. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Yes. CSB tracks, maintains, and reviews POA&M activities on a quarterly basis.
e. OIG findings are incorporated into the POA&M process.	Yes. CSB's POA&M identifies where the weaknesses were identified and clearly states which were found by the OIG.
f. POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	No. The CSB POA&M process does not prioritize the IT security weaknesses. CSB management explained that all of the IT security weaknesses are addressed concurrently.

The ITM is responsible for the development, implementation, and management of the agency wide FISMA POA&M process. The ITM utilizes the POA&M to ensure that control weaknesses, from prior audits/reviews, are addressed and corrected. The ITM, in coordination with the CIO, develops, implements, and manages POA&Ms for the CSB systems. Although CSB is required to report its POA&M progress to OMB on a quarterly basis, CSB last submitted a POA&M to OMB in March 2004. The lack of timely POA&M submissions is because CSB did not fill the ITM position between October 2004 and March 2005.

The POA&M is the authoritative agency management tool used to identify and monitor agency security weaknesses. CSB has an updated POA&M and uses it for tracking corrective actions. Inspection of the current POA&M and discussions with the ITM showed that CSB had not prioritized its IT security weaknesses on the POA&M. Consequently, CSB may not timely address critical weaknesses. In response to this finding, CSB indicated the Agency had prioritized the weaknesses in its September 2005 POA&M submission to OMB. **Finding OIG-IT-04**

Objective 5

Assess the overall quality of the agency's C&A process.

As stated in the FY 2003 and FY 2004 CSB FISMA evaluations, CSB's systems have not been fully certified and accredited. During the course of FY 2004 and 2005, CSB issued an IATO for each of its systems, which authorizes the systems to operate for the period of two years from September 30, 2004. In addition, CSB has obtained contractor assistance to support its certification and accreditation (C&A) efforts. At the time of our FY 2005 FISMA evaluation,

the contractor had completed the initial task of conducting a server audit to support the C&A process; however, the process is not complete. **Finding OIG-IT-01**

Objective 6

Evaluate the status of the following:

a. Is there an agency wide security configuration policy?

b. Identify which software is addressed in the agency wide security configuration policy. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

CSB does not currently have an agency wide security configuration policy. In addition, CSB has not implemented an agency-wide software patch management program and has hired a contractor to correct this deficiency.

During our vulnerability test of CSB's external and internal network infrastructure, we noted the following:

- Externally, CSB has implemented a fail-over firewall configuration to filter out unnecessary network traffic. This firewall mitigates most risks originating from the Internet. However, we noted several vulnerabilities on CSB's external web servers that could be used to gain unauthorized access. This occurred because CSB had not:

  - updated system software with the latest patches/fixes, or

  - disabled unnecessary services/program features.

- Internally, our testes identified vulnerabilities that could possibly lead to unauthorized access. This occurred because CSB had not:

  - updated system software with the latest patches/fixes,

  - secured blank system administration account passwords on workstations, or

  - removed obsolete accounts from the CSB network. For example, we identified 11 user accounts where the user has not logged-on in more than 180 days. **Finding OIG-IT-02**

Objective 7

Evaluate the degree to which the following statements reflect the status:

- **a. The agency follows defined policies and procedures for reporting incidents internally.**
- **b. The agency follows defined policies and procedures for external reporting to law enforcement authorities.**
- **c. The agency follows defined procedures for reporting to the Federal Computer Incident Response Center (FedCIRC) as established by US-CERT. http://www.us-cert.gov.**

CSB's incident reporting program requires the ITM to be informed after: 1) a security violation has occurred, or 2) if the user suspects that there has been a security violation. CSB's main incident reporting process follows US-CERT criteria. CSB has not approved its incident reporting process, but plans to approve the process and procedures during FY 2006.

During FY 2005, CSB had one computer incident related to malicious code. CSB did not notify US-CERT or any external reporting authority because the malicious code was not widespread across the agency. **Finding OIG-IT-05**

Objective 8

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

During FY 2005, CSB implemented a security awareness-training program for its employees, thereby, eliminating a long-standing significant deficiency reported in the FY 2003 and FY 2004 FISMA evaluations. However, the training material does not include information regarding peer-to-peer file sharing. Additionally, at the time of our FY 2005 FISMA review, CSB's ITM did not have adequate security training to perform his duties. However, the ITM has registered for several IT security classes and seminars for early in FY 2006.

Objective 9

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

As previously stated, CSB's security training materials do not currently contain information on peer-to-peer file sharing. To mitigate this deficiency, CSB official indicated the Agency would prepare a separate notification for current employees, and will include specific guidance on peer-to-peer file sharing in updated security awareness documentation.

CSB Privacy Program

OMB encourages IGs to provide any meaningful data they have regarding the agency's privacy program and related activities.

CSB has not developed any privacy specific processes or programs. Accordingly, the OIG has not received any meaningful data and therefore is not able to provide any privacy results for FY 2005.

Appendix A

U.S. Chemical Safety and Hazard Investigation Board FY05 FISMA Report

Micro Agency Reporting Template - IG or Independent Evaluator.

This template should be used by micro-agencies (less than 100 employees) to report to OMB on FISMA Compliance. This template should be submitted to OMB (fisma@omb.eop.gov) no later than October 7, 2005, in accordance with OMB Memo M-05-15 "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

If a micro-agency does not have an IG, Section C requirements should be completed by an independent evaluator.

Please attach any reports or observations from the independent assessment at the time of template submission to OMB.

Name of Agency: **U.S. Chemical Safety and Hazard Investigation Board**
Date: 09/28/2005

Agency systems:		2
Number of agency systems evaluated - by FIPS-199 categorization (high impact, medium impact, low impact, or not yet categorized)	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	2
Of those systems evaluated, number of agency systems certified and accredited, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	0
Of those systems evaluated, number of agency systems with security controls tested FY05, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	0
Of those systems evaluated, number of agency systems with tested contingency plans, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized	0

Micro Agency Reporting Template - IG or Independent Evaluator.

This template should be used by micro-agencies (less than 100 employees) to report to OMB on FISMA Compliance. This template should be submitted to OMB (fisma@omb.eop.gov) no later than October 7, 2005, in accordance with OMB Memo M-05-15 "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

If a micro-agency does not have an IG, Section C requirements should be completed by an independent evaluator.

Please attach any reports or observations from the independent assessment at the time of template submission to OMB.

Name of Agency: **U.S. Chemical Safety and Hazard Investigation Board**
Date: 09/28/2005

Contractor systems:		1
Number of contractor systems evaluated, by FIPS-199 categorization (high impact, medium impact, low impact, or not yet categorized)	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	1
Of those systems evaluated, number of contractor systems certified and accredited, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	0
Of those systems evaluated, number of contractor systems with security controls tested FY05, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	1
Of those systems evaluated, number of contractor systems with tested contingency plans, by FIPS-199 categorization	High Impact:	0
	Moderate Impact:	0
	Low Impact:	0
	Not yet categorized:	0
Number of weaknesses identified in POA&M:		10
Number of weaknesses reported corrected as of 09/28/05:		1

Appendix B

Documentation Used for Evaluation

1. CSB IT Security Plan
2. CIO Appointment Memo for Anna Johnson
3. ISO Appointment Memo for Charlie Bryant
4. Charlie Bryant Resume and Job Description
5. DN American Draft Statement of Work for CSB
6. CSB Staff Directory
7. Draft Computer Security Awareness Training
8. Draft Incident Reporting Policy and Procedures
9. Draft Incident Response Policy and Procedures
10. Federal Incident Reporting Guidelines
11. Interim Authority To Operate (IATO) for CSB's Three Systems
12. CSB Information Technology Contingency Plan
13. Spectra 10000 Information
14. DN American Server Audit
15. IT Department Inventory
16. POA&M, dated July 15, 2005 and POA&M Submission Email
17. Network Topology
18. CSB Agency Structure Chart
19. Sample of Windows XP Configuration Checklists
20. Draft Computer Security Employee Acknowledgement Form
21. Scheduled Training Courses for Charlie Bryant
22. N-Stealth External Scan Against CSB.gov
23. N-Stealth Internal Scan Against Exchange Email Server
24. Vulnerability Assessment Work Paper and Results
25. CSB 2004 IT Capital Plan
26. DN American Weekly Report