OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2006)

Report No. 2007-P-00019

April 23, 2007

U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00019
April 23, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) information security program complies with the Federal Information Security Management Act (FISMA). We also sought to determine whether CSB complied with Office of Management and Budget (OMB) Memorandum M-06-16 requirements for protecting sensitive information.

Background

The Office of Inspector General (OIG) contracted with KPMG, LLP to assist in performing the Fiscal Year 2006 FISMA independent evaluation of the CSB information security program, and the Agency's efforts to protect its sensitive information. This evaluation adheres to the OMB reporting guidance for micro-agencies, which CSB is considered.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2007/20070423-2007-P-00019.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2006)

What KPMG Found

In Fiscal Year 2006, CSB made significant changes that enhanced the security of information system resources. CSB reorganized its Information Technology department by promoting and hiring key management officials. CSB also consolidated three information system functions into one Agency-owned General Support System (GSS) that mitigated a portion of the prior year weakness related to the implementation of security controls. The new GSS was certified and accredited for the operating environment. Further, CSB took steps to correct all of the security weaknesses identified during Fiscal Year 2005. However, KPMG found areas where CSB could further strengthen its information security program. KPMG found that:

- CSB's new consolidated GSS Security Plan did not address many of the Federal requirements prescribed by the National Institute of Standards and Technology. CSB also had not tested the new GSS' security controls for effectiveness. In addition, CSB had not assigned a risk categorization to the GSS in accordance with Federal requirements.
- While CSB reported a computer theft to the Federal Protective Service and the local police department, the incident was not reported to the United States Computer Emergency Readiness Team. Additionally, the theft was not documented in a formal incident report as required by CSB policy.
- CSB had not identified or implemented policies and procedures that address the protection of sensitive personally identifiable information.
- Although checklists are used to set up computers, there is no policy that mandates the use of the checklists, and the checklists did not contain security configuration settings. In addition, CSB had not developed an Agency-wide security configuration policy.
- CSB had not tested the GSS' contingency plan during Fiscal Year 2006 and the content of the plan needs improvement. Further, CSB had not conducted an e-authentication risk assessment.

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

OFFICE OF
INSPECTOR GENERAL

April 23, 2007

MEMORANDUM

SUBJECT: Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2006) Report No. 2007-P-00019

FROM: Patricia H. Hill
Assistant Inspector General for Mission Systems

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

Attached is KPMG, LLP's 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. Environmental Protection Agency's Office of Inspector General. The report also includes KPMG's completed Fiscal Year 2006 Federal Information Security Management Act Reporting Template, as prescribed by the Office of Management and Budget (OMB).

In accordance with OMB reporting instructions, the Office of Inspector General is forwarding this report to you for submission, along with your Agency's required information, to the Director, OMB.

If you or your staff has any questions, please contact me at 202-566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Evaluation Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information

(Fiscal Year 2006)

April 23, 2007

Abbreviations

ATO	Authority to Operate
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
GSS	General Support System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SP	Special Publication
SSL	Secure Socket Layer
VPN	Virtual Private Network
US-CERT	United States Computer Emergency Readiness Team

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2006)

Table of Contents

Chapters

Chapter 1
Executive Summary

Introduction

The Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) tasked KPMG to conduct a review of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act (FISMA) and the requirements to protect agency sensitive information as prescribed by Office of Management and Budget (OMB) Memorandum M-06-16. CSB is a small federal entity and does not have an extensive information security program and related practices comparable to those of larger federal entities. This was 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 and privacy program and practices. In addition, we reviewed documentation supporting security training, security-related information technology (IT) capital planning efforts, memoranda regarding information security policies, and plans for future information security assessments. Through inspection of the documentation received and inquiry with CSB personnel, we evaluated CSB's progress in meeting performance measures prescribed by OMB.

Reporting Requirements

OMB has issued FISMA reporting guidance for "micro-agencies", which OMB defines as an agency that has 100 employees or less. CSB meets the OMB criteria for a micro-agency. Appendix A contains the results of our evaluation in accordance with the micro-agencies report format. The EPA OIG requested that KPMG review the CSB information security program in more detail than required by the FISMA micro-agency reporting guidance.

The June 23, 2006 OMB memorandum required agencies to assess their baseline activities regarding the protection of sensitive Agency information. OMB required agencies to apply safeguards outlined by a National Institute of Standards and Technology (NIST) checklist. This checklist outlined multiple Action Steps and Action Items intended to compensate for the lack of physical security controls when information is removed from or accessed from outside the agency location. OMB requested that the Inspectors General community help to assess the status of their agencies' safeguards. In conjunction with the FY 2006 FISMA review, we assessed CSB's progress in implementing the prescribed safeguards. Consequently, this report contains additional details on our observations regarding CSB's information security program and efforts to protect sensitive information.

Results in Brief

The CSB IT department underwent significant changes during FY 2006. As such, CSB:

- Reorganized the IT department by promoting the Information Technology Manager to IT Director, and hired both a Deputy IT Director and an IT Specialist.
- Consolidated its three information system functions, (Investigation, Recommendation and Technical Solutions, and Administrative Functions), into one agency-owned General Support System (GSS).
- Certified and accredited the new GSS.

In addition, to assist in the remediation of the previously identified weaknesses, the Chief Information Officer (CIO) hired a contractor. As such, CSB took action to correct many of the previously identified security weaknesses and we have closed the five prior year findings. Table 1 contains a summary of the FY 2005 findings.

Table 1. Summary of FY 2005 Findings

FY 2005 FISMA Finding	Status	Notes
FY05-OIG-IT-01 Security Certification and Accreditation (C&A)	Action Completed	The GSS has been certified and accredited and granted a full authority to operate.
FY05-OIG-IT-02 Security Control Implementation	Administratively Closed	CSB consolidated its three systems into one consolidated GSS to mitigate a portion of the FY 2005 finding. This consolidation included the update and installation of new hardware and software. During FY06, CSB indicated that it did not test the security controls of the old system because it was being replaced. Therefore, this finding was administratively closed. See FISMA finding FY06-OIG-IT05 for the results of our FY06 evaluation of the security control implementation for the new consolidated GSS.
FY-05-OIG-IT-03 Security Training	Action Completed	CSB updated its security awareness documentation to include a slide that provides information on the Agency's policy that prohibits the use of peer-to-peer file sharing software on CSB's network. The updated training has been completed by CSB personnel.
FY05-OIG-IT-04 Security Program Management	Action Completed	An IT Director has been assigned. Additionally, POA&Ms are being submitted as required and used to track and prioritize corrective actions.

FY 2005 FISMA Finding	Status	Notes
FY05-OIG-IT-05 Security Incident Handling	Action Completed	CSB developed and approved its incident response and reporting policies.

Although CSB made improvements by its reorganization, consolidation, and commitment to remediate its security weaknesses, our FY 2006 evaluation identified areas requiring additional management emphasis. Table 2 summaries the significant deficiencies identified during this year's review.

Table 2. Summary of FY 2006 Findings

FY 2006 FISMA Finding	Status	Remarks	Recommendation
FY06-OIG-IT-01 C&A Process	Open	The new consolidated GSS Security Plan did not address many of the federal requirements prescribed by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems.* In addition, CSB has not assigned a risk categorization to the GSS in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems.*	CSB should: 1. Update the new GSS' Security Plan to include all major categories as prescribed by NIST SP 800-18. 2. Assign a risk categorization to the new consolidated GSS in accordance with FIPS 199 and NIST SP 600-60. 3. Schedule and conduct a test of the security controls for the new consolidated GSS. For each weakness identified, management should either (1) develop and implement corrective actions or (2) document its decision to accept the related risk to the system's operation as residual.
FY06-OIG-IT-02 Security Incident Reporting	Open	During FY 2006, a computer theft occurred at CSB headquarters. CSB reported the theft to the Federal Protective Service and the local police department. However, CSB did not report the incident to the United States Computer Emergency Readiness Team (US-CERT) and document a formal incident report.	CSB should: 4. Initiate action to remind employees about the importance of reporting computer security incidents.

FY 2006 FISMA Finding	Status	Remarks	Recommendation
FY06-OIG-IT-03 Personally Identifiable Information	Open	CSB had not identified or implemented any policies and procedures, which address the protection of sensitive personally identifiable information (PII).	CSB should: 5. Review the Agency's PII program using the security checklist and guidelines as prescribed by OMB Memorandum 06-16. 6. Create POA&Ms for all identified weaknesses.
FY06-OIG-IT-04 System Configuration and Patch Management	Open	CSB does not currently have an agency wide security configuration policy. Our vulnerability test results disclosed weaknesses on CSB's external and internal servers that could be used to gain unauthorized access. CSB could have prevented many of these weaknesses had it implemented configuration and patch management processes. Additionally, although checklists are used to setup computers, there is no policy, which mandates the use of the checklists, nor did the checklists contain security configuration settings.	CSB should: 7. Develop and implement an Agency-wide security configuration policy. 8. Update the newly published Patch Management and System Update policy to include steps for ensuring newly implemented systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production. 9. Implement procedures to ensure that new systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production. 10. Establish and implement a policy and procedure that mandates the IT department use the System Setup Checklist to set up new computers. 11. Update the System Setup Checklist to include the CSB required security configuration settings.
FY06-OIG-IT-05 Security Control Implementation	Open	CSB has not tested the GSS' contingency plan during FY 2006. Furthermore, the	CSB should: 12. Establish a POA&M to conduct a test of the GSS'

FY 2006 FISMA Finding	Status	Remarks	Recommendation
		content of the GSS contingency plan needs improvement and finally, CSB has not conducted an e-authentication risk assessment.	contingency plan. 13. Conduct and document the results of the test of the GSS' contingency plan. 14. Update the GSS' contingency plan to include all the required major areas as prescribed by NIST SP 800-34. 15. Conduct an e-authentication risk assessment.

Chapter 2
Results of Independent Evaluation

Objective 1 - Evaluate a Representative Subset of Systems

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 Federal Information Processing Standard (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
Agency Systems	
High Impact	0
Moderate Impact	0
Low Impact	0
Not Categorized	1
Contractor Systems	
High Impact	0
Moderate Impact	0
Low Impact	0
Not Categorized	0
Total Systems	**1**

CSB assigned risk categorizations to each sub-system of its consolidated GSS. However, the GSS, as a whole, has not been assigned a risk categorization according to the FIPS 199[1] criteria. **Finding FY06-OIG-IT-01**

Recommendation

CSB should:

- Assign a risk categorization to the new consolidated GSS in accordance with FIPS 199 and NIST SP 600-60.

[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.

Objective 2 - Actual Performance by Risk Impact Level

Identify actual performance in FY 2006 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 and evaluated within the past year.

Security Category	Total Number
Total number certified and accredited	1
Total number with security controls tested and evaluated	0
Total number with contingency plan tested	0

While the CSB GSS has a certification and accreditation (C&A) package current as of FY 2006, the security controls on the system had not been tested and evaluated against NIST Special Publication 800-26[2] or 800-53[3]. Although CSB conducted risk assessments to identify weaknesses in its systems, CSB had not conducted security tests and evaluations to determine whether implemented security control measures (1) adequately protected CSB's systems or (2) worked as intended. CSB should select an initial set of security controls for the new GSS, document the agreed-upon set of security controls in the GSS security plan, and conduct a test to ensure the security are effective. The initial set of security controls should include a broad range of Managerial, Operational, and Technical security controls. **Finding FY06-OIG-IT-01.**

Additionally, CSB had not tested its contingency plan during FY 2006. Furthermore, our review disclosed that CSB could improve its contingency planning efforts in the following areas: (1) identifying roles and responsibilities, (2) identifying support resources, (3) outlining procedures for restoring critical applications, (4) arranging for alternate processing facilities, and (5) documenting requirements for periodic contingency plan testing, test results and analyses. **Finding FY06-OIG-IT-05.**

---

[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.

Recommendations

CSB should:

- Schedule and conduct a test of the security controls for the new consolidated GSS. For each weakness identified, management should either (1) develop and implement corrective actions or (2) document its decision to accept the related risk to the system's operation as residual.
- Establish a POA&M to conduct a test of the GSS' contingency plan.
- Conduct and document the results of the test of the GSS' contingency plan.
- Update the GSS' contingency plan to include all the required major areas as prescribed by NIST SP 800-34.

Objective 3 - Oversight of Systems and System Inventory

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.	**Not applicable**; CSB does not have any systems owned or operated by contractors.
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.	**Approximately 96-100%**; CSB maintains a complete list of all systems. CSB has no national security systems.
c. The OIG generally agrees with the CIO on the number of agency owned systems.	**Yes**; the EPA OIG generally agrees with the CIO concerning the number of information systems.
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**; the EPA OIG generally agrees that no information systems are used or operated by contactors.
e. The agency inventory is maintained and updated at least annually.	**Yes**; the agency inventory is maintained and updated at least annually.
f. The agency has completed system e-authentication risk assessments.	**No**; e-authentication risk assessments have been conducted during FY 2006.

During FY 2006, CSB consolidated its three systems (including the one contractor system) into one agency-owned GSS, which has multiple sub-systems. Additionally, CSB tracks its IT inventory using a commercial off-the-shelf database. With this database, CSB has the ability to query specific IT equipment. CSB updates the database

at least annually or when changes/deletions are needed. Finally, the CSB has informally notified the EPA OIG of the number of systems operational at CSB, and the EPA OIG generally agrees with the CSB system consolidation.

During our evaluation, we determined that an e-authentication risk assessment was not completed during FY 2006. **Finding FY06-OIG-IT-05**

Recommendation

CSB should:

- Conduct an e-authentication risk assessment.

Objective 4 - Plan of Action and Milestones Status

Assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestones (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**; program officials report directly to the IT Director, 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**; the POA&M process identifies whether findings 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.	**Yes**; the POA&M process prioritizes the IT security weaknesses.

The IT Director, in coordination with the CIO, develops, implements, manages, and prioritizes POA&Ms. We concluded that the IT Director utilizes the POA&M process to ensure that control weaknesses from prior audits/reviews are addressed and corrected. During FY 2006, CSB regularly submitted the POA&M to OMB on a quarterly basis.

Objective 5 - Agency Certification and Accreditation Process

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

Evaluate the Status of the Following	Results
Assess the overall quality of the agency's C&A process	**Satisfactory**

CSB corrected a long-standing deficiency from the FY 2003 and FY 2004 CSB FISMA evaluations by completing the C&A of its systems. During FY 2006, CSB consolidated its three information system functions (Investigation, Recommendation and Technical Solutions, and Administrative Functions) into one agency-owned GSS. We noted that the new consolidated GSS was certified and accredited in FY 2006 and granted a full authority to operate. However, CSB had not conducted a test of the GSS security controls to determine whether the implemented security controls were effective.

During our review of the C&A process, we obtained the C&A package, which consisted of: the GSS' security plan, the CSB IT Risk Assessment External Review report, and the POA&M report. Our review of the GSS security plan, for adherence with federal requirements[4], identified that the plan did not address some of the required elements. These missing elements included:

- A list of laws, regulations, or policies that establish specific requirements for the confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system;
- Titles of security controls;
- Descriptions of how security controls are being implemented or planned to be implemented;
- Clear identification of system controls as common security controls or system-specific controls;
- Indication of the party responsible for implementing identified security controls; and
- Address of the system owner, authorizing official and other designated contacts. **Finding FY06-OIG-IT-01**

[4] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, outlines the requirements that must be documented in a system security plan and NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides the guidelines that enable more consistent, comparable, and repeatable assessments of security controls in federal information systems.

During our review of the risk assessment report provided as a part of the GSS C&A package, we noted that the impact analysis performed was not conducted in accordance with FIPS 199.

We assessed the overall quality of CSB's C&A process as satisfactory based upon noted deficiencies in the new consolidated GSS' C&A package components and our determination that security controls for the system have not been tested (as discussed in Objective 2).

Recommendation

CSB should:

- Update the new GSS' Security Plan to include all major categories as prescribed by NIST SP 800-18.

Objective 6 - Agency Wide Security Configuration Policy

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.

Evaluate the Status of the Following	Results
a. Is there an agency wide security configuration policy	**No**
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.	**Not Applicable** - CSB does not have an Agency-wide security configuration policy.

During our FY 06 evaluation, CSB approved its patch management, system update, and encryption policies, and we did not review the policies and implementation. However, CSB should place more emphasis on defining, and implementing security configuration settings. In particular:

- CSB does not have an Agency-wide configuration policy.
- CSB does not have a formal policy that mandates the use of the Computer Setup Checklist for all new computer installations. In addition, the checklist does not specify the CSB require security configuration settings.

In addition, our vulnerability test results disclosed weaknesses on CSB's external and internal servers that could be used to gain unauthorized access. CSB could have prevented many of these weaknesses had it implemented configuration and patch management processes to ensure:

- unnecessary system services and program features are disabled,
- servers and network devices are securely configured,
- system software are updated with necessary patches/fixes,
- systems do not run obsolete software no longer supported by the vendor, and
- users are forced to change passwords that are older than 90 days. **(FY06-OIG-IT-04)**

Recommendations

CSB should:

- Develop and implement an Agency-wide security configuration policy.
- Update the newly published Patch Management and System Update policy to include steps for ensuring newly implemented systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production.
- Implement procedures to ensure that new systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production.
- Establish and implement a policy and procedure that mandates the IT department use the System Setup Checklist to set up new computers.
- Update the System Setup Checklist to include the CSB required security configuration settings.

Objective 7 - Incident Reporting

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.

Evaluate the Status of the Following	Results
a. The agency follows defined policies and procedures for reporting incidents internally.	**No**
b. The agency follows defined policies and procedures for external reporting to law enforcement authorities.	**No**
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.	**No**

CSB's incident reporting program requires the IT Director to be informed: 1) after 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. Through discussion with CSB management, we determined that the Incident Response and Reporting Policies were developed by the IT Director and approved per the Information Security Program**.**

During FY 2006, CSB had one computer incident related to theft of property. While CSB notified the Federal Protective Service and the District of Columbia (DC) Police Department, US-CERT was not notified. Although the Information Technology Security Officer (ITSO) was alerted of the incident, the CSB Incident Reporting Form, which is prescribed by the Information Security Incident Reporting Procedure, was not completed for the incident. **Finding FY06-OIG-IT-02**

Recommendation

CSB should:

- Initiate action to remind employees about the importance of reporting computer security incidents.

Objective 8 - Security Training and Awareness Program

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

Evaluate the Status of the Following	Results
Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?	**Yes**; CSB has conducted security training and awareness for all employees including contractors and those employees with significant IT security responsibility.

During the FY 2006 review, we confirmed that all CSB employees and contractors had received security awareness training. We also determined that the IT Director and staff with significant security responsibilities have completed training in FY 2006 and are enrolled in certification training classes and other seminars for FY 2007.

Objective 9 - Peer-to-Peer File Sharing Policy

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

Evaluate the Status of the Following	Results
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	**Yes**; peer-to-peer file sharing is addressed in the security awareness training at CSB.

In FY 2005, we identified that CSB's policy regarding peer-to-peer file sharing was not included in the Agency wide training. To correct the prior year finding, CSB updated the security awareness documentation to include a slide that includes information on the Agency's policy that prohibits the use of peer-to-peer file sharing software on CSB's network. During the current year's review, we verified that CSB personnel had completed the updated training and consequently received information on peer-to-peer file sharing. (see Objective 8).

Controls over Sensitive Agency Information

CSB is required by OMB to adhere to the information security requirements prescribed in Memorandum M-06-16, Protection of Sensitive Agency Information.

CSB has not identified or implemented any policies and procedures which explicitly address the protection of sensitive agency information. Existing policies address remote access to PII through Virtual Private Networks and Secure Socket Layer, but does not address PII that is physically removed. Additionally, the four recommended actions in OMB Memorandum M-06-16 have been partially implemented. Appendix B contains the results of the PII evaluation. **Finding FY06-OIG-IT-03**

Recommendations

CSB should:

- Review the Agency's PII program using the security checklist and guidelines as prescribed by OMB Memorandum 06-16.

- Create Plans of Action and Milestone (POA&M) for all identified weaknesses.

CSB Management Response and KPMG's Comments

In general, CSB management agreed with the report's findings and recommendations. CSB provided a corrective action plan with action steps and milestone dates. Subsequent to receiving CSB management's response, CSB also provided a corrective action plan regarding the testing of the controls for the new GSS. CSB indicated it would complete the testing by September 30, 2007. In our opinion, CSB proposed actions when implemented would adequately address the report's recommendations. Appendix C contains CSB's response to the draft report.

Appendix A

Micro Agency Reporting Template

U.S. Chemical Safety and Hazard Investigation Board FY 2006 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 1, 2006.

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.

U.S. Chemical Safety and Hazard Investigation Board
03/15/2007

Agency systems:		0
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:	1
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:	1
Of those systems evaluated, number of agency systems with security controls tested FY06, 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 1, 2006.

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.

U.S. Chemical Safety and Hazard Investigation Board
03/15/2007

Contractor systems:		0
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:	0
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:	0
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 the POA&M:		8
Number of weaknesses reported corrected as of 9/30/06:		6

IG DATA COLLECTION INSTRUMENT

This data collection instrument (DCI) was developed by the Federal Audit Executive Council (FAEC) Information Technology (IT) Committee of the President's Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency (ECIE) to assist Inspectors General (IGs) in determining their Agency's compliance with Office of Management and Budget (OMB) Memorandum M-06-16. The data collection instrument contains three parts. The first part is based on a security checklist developed by the National Institute of Standards and Technology (NIST) (see Section 1 below). Questions in the DCI are designed to assess Agency requirements in the memorandum, which are linked to NIST Special Publication (SP) 800-53 and 800-53A. Each IG can use the associated checklist and the relevant validation techniques for their own unique operating environment. Section 2 is the additional actions required by OMB M-06-16. Section 3 should document your overall conclusion as well as detailed information regarding the type of work completed and the scope of work performed.

For each overall Step and Action Item, please respond **yes, no, partial, or not applicable**. For no, partial, and not applicable responses, please provide additional information in the comments sections. After the yes, no, partial, or not applicable response, IGs have the option to provide an overall response using the six control levels as defined below for the overall Step. Each condition for the lower level must be met to achieve a higher level of compliance and effectiveness. For example, for the control level to be defined as "Implemented", the Agency must also have policies and procedures in place. The determination of the control level for each Step should be based on the responses provided to the Action Items included in that Step.

Controls Not Yet in Place - The answer would be "Controls Not Yet in Place" if the Agency does not yet have documented policy for protecting personally identifiable information (PII).

Policy - The answer would be "Policy" if controls have been documented in Agency policy**.**

Procedures - The answer would be "Procedures" if controls have been documented in Agency procedures**.**

Implemented - The answer would be "Implemented" if the implementation of controls has been verified by examining procedures and related documentation and interviewing personnel to determine that procedures are implemented**.**

Monitored & Tested - The answer would be "Monitored & Tested" if documents have been examined and interviews conducted to verify that policies and procedures for the question are implemented and operating as intended.

Integrated - The answer would be "Integrated" if policies, procedures, implementation, and testing are continually monitored and improvements are made as a normal part of Agency business processes.

PLEASE PROVIDE YOUR RESPONSES USING THE DROP DOWN MENU IN GRAY		
Section One		
Security Controls and Assessment Procedures		
Security Checklist For Personally Identifiable Information That Is To Be Transported		
and/ or Stored Offsite, Or That Is To Be Accessed Remotely	**REQUIRED RESPONSE**	**OPTIONAL RESPONSE**
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitored & Tested***
		Integrated
STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?	*No*	
Action Item 1.1: Has the Agency verified information categorization to ensure identification of personal identifiable information requiring protection when accessed remotely or physically removed?	*No*	
Comments: The Agency has not verified information categorization to include PII.		
Action Item 1.2: Has the Agency verified existing risk assessments?	*No*	
Comments: The Agency has not verified existing risk assessments to include PII.		
OVERALL STEP 1 COMMENTS: The Agency has not yet identified all PII.		
	REQUIRED RESPONSE	**OPTIONAL RESPONSE**
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitored & Tested***
		Integrated
STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?	*Partial*	
Action Item 2.1: Does existing Agency policy address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	*Partial*	
Comments: CSB has addressed the remote access controls concerning the Time & Attendance GSS sub-system, but has not addressed the PII on a Senior Agency Personnel's laptop. Physically removed PII has not been addressed.		

Action Item 2.2: Does the existing Agency organizational policy address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	Partial	
y identifiable information physically removed:		
y explicitly identify the rules for determining whether physical	No	
1. For personall y identifiable information that can be removed, does the policy	No	
ypted and that appropriate procedures, training		
a. Does the polic y measures are in place to ensure that remote use of this		
ypted information does not result in bypassing the protection provided by		
b. For personall yption?		
require that information be encr y identifiable information accessed remotely:		
and accountabilit y explicitly identify the rules for determining whether remote	Yes	
encr		
the encr		
2. For personall		
y require that this access be	Yes	
a. Does the polic (VPN) connection established using		
gency-issued authentication certificate(s) or hardware tokens?		
access is allowed?		
b. When remote access is allowed, does the polic y identify the rules for	No	
g whether download and remote storage of the information is		
accomplished via a virtual private network (For example, the policy could permit remote access to a database,		
A g and local storage of that database.)		
c. When remote access is allowed, does the polic		
determinin		
allowed?		
but prohibit downloadin		

Comments: The CSB Information System Security Plan does not address the removal of PII, including: encryption, procedures, training, and accountability measures to address that PII encryption controls can not be bypassed. While the CSB Information System Security Plan does not explicitly state the systems that contain PII data, the document identifies the types of remote access allowed to each GSS sub-system. As stated in the Plan, the Time & Attendance sub-system can only be accessed through VPN and a SSL encrypted connection for Remote Access (RA) users, which uses an agency-issued authentication certificate. Lastly, the Plan does not identify rules for determining whether download and remote storage of the information is allowed.

Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?	No	
Comments: Organizational policies have not been revised and developed to adequately address PII.		
OVERALL STEP 2 COMMENTS: The CSB Information System Security Plan does not include specific requirements for: 1) encryption, procedures, training, and accountability measures to address that PII encryption controls can not be bypassed, 2) PII considerations for the Senior Agency Personnel's laptop, 3) encrypting backup media containing PII that is transported and/or stored offsite, and 4) identifying rules for determining whether download and remote storage of the information is allowed.		

		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitored & Tested***
		Integrated
STEP 3: Has the Agency implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level?	*No*	
Action Item 3.1: In the instance where personally identifiable information is transported to a remote site, have the NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form been implemented?	*No*	
Comments:		
** Evaluation could include an assessment of tools used to transport PII for use of encryption.* *Action Item 3.2: In the instance where PII is being stored at a remote site, have the NIST SP 800-53 security controls ensuring that information is stored only in encrypted form been implemented?*	*No*	
Comments: The Agency has not yet identified all instances when backup media that contain PII is being stored at remote sites and whether storage methods use encryption. ** Evaluation could include a review of remote site facilities and operations.*		
OVERALL STEP 3 COMMENTS: The Agency has not yet identified all instances where PII is being transported and/or stored offsite. Additionally, the Agency has not implemented encryption on their back-up media that is transported and stored offsite.		
If personally identifiable information is to be transported and/or stored offsite		
follow Action Item 4.3, otherwise follow Action Item 4.4		

	REQUIRED RESPONSE	OPTIONAL RESPONSE
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitored & Tested***
		Integrated
STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?	*No*	
Action Item 4.1: Have NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection been implemented by the Agency?	*No*	
Comments:		
Action Item 4.2: Have the NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information been enforced by the Agency?	*No*	
Comments:		
If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.		
Action Item 4.3: Have the NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information been implemented by the Agency?		
	No	
Comments:		
Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?	*No*	
Comments:		
OVERALL STEP 4 COMMENTS: The Agency has not yet identified all instances where PII is being accessed remotely.		
(The source for all the control steps above is NIST SP 800-53 and SP 800-53A assessment procedures.)		

** Evaluation could include a review of the configuration of VPN application(s).*

** Evaluation could include a review of controls for downloading PII.*

Section Two		
Additional Agency Actions Required by OMB M-06-16		
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitored & Tested***
		Integrated
1. Has the Agency encrypted all data on mobile computers/devices which carry Agency data unless the data is determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?	*No*	
Comments: Data is not encrypted on mobile computers or devices which carry agency data.		
2. Does the Agency use remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access?	*No*	
Comments: Currently, only username and password combinations are used utilized when gaining access to the CSB network; separate devices are not implemented to provide two-factor authentication.		
3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?	*Yes*	
Comments: CSB's VPN Concentrator is configured to time-out users after 30 minutes of inactivity.		
4. Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data has been erased within 90 days or its use is still required?	*Partial*	
Comments: CSB logs data extracted from databases holding sensitive information, but retains the information on a laptop indefinitely.		

Section Three					
To assist the PCIE/ECIE in evaluating the results provided by individual IGs and in creating the government-wide response, please provide the following information:					
Type of work completed (i.e., assessment, evaluation, review, inspection, or audit).					
OIG Response: Review, as part of the annual FISMA review					
Scope and methodology of work completed based on the PCIE/ECIE review guide Step 2 page 4. *(Please address the coverage of your assessment, and include any comments you deem pertinent to placing your results in the proper context.)*					
OIG Response: We conducted focused interviews with the Chemical Safety Board staff. We also reviewed: 1) The Statement of Work and First Federal Contract for Off-Site Data Storage, 2) CSB Information System Security Plan, 3) Screenshot of VPN and Domain Authentication Screens, 4) Screenshot of the SSL Connection to Track-IT, 5) Screenshot of the idle timeout setting on the VPN concentrator, 6) CSB Patch Management & Encryption Policy, approved in FY 2007, 7) Five Time & Attendance Extraction Logs, and 8) CSB PII FY2006 FISMA Submission.					
Assessment Methodologies Used to Complete the DCI Sections					
	Mark All That Apply				
	Section One				**Section Two**
	Step 1	**Step 2**	**Step 3**	**Step 4**	
Interviews (G/F/C)	**G**	**G**	**G**	**G**	**G**
Examinations (G/F/C)	**G**	**G**	**G**	**G**	**G**
Tests (independently verified - Y/N)	**Y**	**Y**	**Y**	**Y**	**Y**
Assessment Method Descriptions consistent with NIST SP 800-53A - Appendix D pages 34 - 36.					
***G** = Generalized. **F** = Focused. **C** = Comprehensive. **Y** = Yes. **N** = No.*					

Overall Summary Statement. (Please refer to page five of the review guide for sample language for summary statements.)					
Based on our assessment, we found that the agency has not identified or implemented any policies and procedures which explicitly address the protection of sensitive personal information. Upon inspection of the CSB Information System Security Plan, we noted that the existing policy addresses remote access to PII through VPN and SSL, but does not address PII that is physically removed. Because PII has not been formally identified, Steps 3 and 4 were unable to be completed.					
The agency needs to improve in the following areas:					
~ Identify all information with PII					
~ Ensure policies include specific requirements for: 1) physical removal of PII, 2) encryption, procedures, training, and accountability measures to address that PII encryption controls can not be bypassed, 3) the download and remote storage of PII, 4) encryption of all data on mobile computers/devices, 5) two-factor authentication where one of the factors is provided by a device separate from the computer gaining access, and 6) logs for the extraction of computer-readable data from databases holding sensitive information, including verification that each extract has been erased within 90 days or its use is still required.					

Appendix C

CSB's Response to Draft Report

U.S. 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

Carolyn W. Merritt
Chairman & CEO
John S. Bresland
Gary L. Visscher
Board Member
William B. Wark
Board Member
William E. Wright
Board Member

March 9, 2007

Rudolph Brevard
Director, Information Resource Management Assessments
U.S. Environmental Protection Agency
Office of Inspector General
1200 Pennsylvania Ave. (2421T)
Washington DC 20460

Dear Mr. Brevard:

Thank you for the independent evaluation of the U.S. Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Management Act (FISMA) and efforts to protect sensitive agency information. As reported, the CSB made progress in fiscal year (FY) 2006 in completing actions on prior year FISMA findings. This was accomplished in part, by consolidating three old systems into one General Support System, and updating and installing new hardware and software.

Although we made significant progress in improving our information systems and security during FY 2006, we agree with the findings summarized in the revised Tables 1 & 2 you provided. Attached is an updated Table 2 with our planned actions to address each finding and milestones for completion. Further, we will update our Plan of Actions and Milestones, which will be submitted to the Office of Management and Budget later this month, to include the planned actions for each of the open findings. Please contact Anna Johnson at 202-261-7639, or Charlie Bryant at 202-261-7666 for further information on any of these items.

Sincerely,

/s/

Carolyn W. Merritt
Chairman & CEO

Attachment

Attachment

Summary of FY 2006 Findings & CSB Planned Actions

FY 2006 FISMA Finding	Status	Planned Actions
FY06-OIG-IT-01 C&A Process	Open	**By April 30, the CSB will:** 1. Update the new GSS' Security Plan to include all major categories as prescribed by NIST SP 800-18. 2. Assign a risk categorization to the new consolidated GSS in accordance with NIST FIPS 199 and NIST SP 600-60.
FY06-OIG-IT-02 Security Incident Reporting	Open	**By March 31, the CSB will:** 3. Update Incident Reporting and Response Procedures to include reporting to US-CERT.
FY06-OIG-IT-03 Personally Identifiable Information	Open	**By July 31, the CSB will:** 4. Conduct an assessment in accordance with Office of Management and Budget memorandum 06-16 and 06-19; based on the assessment, develop necessary policies and procedures. 5. Update quarterly POA&M for all identified weaknesses.

Attachment

Summary of FY 2006 Findings & CSB Planned Actions

FY 2006 FISMA Finding	Status	Planned Actions
FY06-OIG-IT-04 System Configuration and Patch Management	Open	**By July 31, the CSB will:** 6. Develop and implement an Agency-wide Security Configuration Policy. The policy will include: a. Procedures to ensure that new systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production. b. Procedures that mandate the IT department use the System Setup Checklist to set up new computers and servers. 7. Update the newly published Patch Management and System Update policy to include steps for ensuring newly implemented systems are (1) updated to the latest software versions and (2) tested for known vulnerabilities before being placed into production. 8. Update the System Setup Checklist to include the CSB required security configuration settings.
FY06-OIG-IT-05 Security Control Implementation	Open	**By August 31, the CSB will:** 9. Add item to CSB quarterly POA&M to conduct a test of the GSS' contingency plan. 10. Conduct and document the results of the test of the GSS' contingency plan. 11. Update the GSS' contingency plan to include all the required major areas as prescribed by NIST SP 800-34. 12. Conduct an e-authentication risk assessment.