OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2007)

Report No. 08-P-0134

April 21, 2008

08-P-0134
April 21, 2008

U.S. Environmental Protection Agency
Office of Inspector General

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The review was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB)'s information security program compliance with the Federal Information Security Management Act (FISMA). Where appropriate, we also sought to make recommendations to ensure a security framework is in place that is capable of meeting security requirements into the future.

Background

CSB contracted with Total Systems Technologies Corporation (TSTC) to assist in performing the Fiscal Year 2007 FISMA assessment under the direction of the U.S. Environmental Protection Agency Office of Inspector General. The review adhered to the Office of Management and Budget reporting guidance for micro-agencies, which CSB is considered, and included an assessment of CSB progress in protecting its sensitive information, including Personally Identifiable Information.

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/2008/20080421-08-P-0134.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 2007)

What TSTC Found

During Fiscal Year 2007, CSB continued to make progress in improving the security of its information system resources. CSB had done this by performing the following:

- assigning a risk categorization to CSB's General Support System in accordance with Federal requirements,
- developing policies mandating the use of security configuration checklists and updating them to contain security configuration settings, and
- conducting contingency plan testing and an e-authentication risk assessment.

CSB has also taken the steps necessary to allow CSB management to align the organization's security program with the Personally Identifiable Information changes directed by the Office of Management and Budget. Further, CSB took the necessary steps to complete all but one of the planned actions in response to the security weaknesses identified during Fiscal Year 2006 audit.

What TSTC Recommends

TSTC did find areas where CSB could continue to improve its information security program. Specifically, TSTC recommends that CSB:

- Expand the security training to include specialized, role-based training.
- Document the CSB Breach Policy and related privacy information policies and procedures to meet CSB needs and Office of Management and Budget requirements.
- Update the CSB security policy and associated procedures to address reviewing, approving, and documenting non-standard security configurations.
- Update, as applicable, the appropriate security documentation to ensure compliance with National Institute of Standards and Technology Special Publication 800-53 controls guidance.

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

OFFICE OF
INSPECTOR GENERAL

April 21, 2008

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 2007)
Report No. 08-P-0134

FROM: Rudolph M. Brevard Rudolph M. Brevard
Director, Information Resources Management Assessments

TO: The Honorable John. S. Bresland
Chairman and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board

This final report on the above subject area synopsizes the results of information technology security work performed by Total Systems Technologies Corporation (TSTC) under the direction of the U.S. Environmental Protection Agency's Office of Inspector General (OIG). The report also includes TSTC's completed Fiscal Year 2007 Federal Information Security Management Act Reporting Template, as prescribed by the Office of Management and Budget (OMB).

The estimated cost for the OIG performing contract management oversight is $3,235. This cost does not include the contracting service costs, which was funded by the U.S. Chemical Safety and Hazard Investigation Board.

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 of OMB.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0893 or brevard.rudy@epa.gov.

U.S. Chemical Safety and
Hazard Investigation Board

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 2007)

March 31, 2008

U.S. Chemical Safety and
Hazard Investigation Board

REPORT CONTRIBUTORS

Thomas Gangi, TSTC, Project Manager
Mark Podracky, TSTC, Subject Matter Expert (Alternate Project Manager)

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
FY	Fiscal Year
GSS	General Support System
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
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

U.S. Chemical Safety and
Hazard Investigation Board

March 31, 2008

Patricia Hill, Assistant Inspector General for Mission Systems
The U.S. Environmental Protection Agency
Office of the Inspector General
1200 Pennsylvania Avenue, NW
Washington, DC 20460

Subject: Evaluation of U.S. Chemical Safety and Hazard Investigation Board's (CSB) Compliance with the Federal Information Security Management Act (FISMA) 2002 for Fiscal Year 2007 Evaluation Report

Ms. Hill:

Attached is the Total Systems Technologies Corporation (TSTC) report on the above subject area. This report synopsizes the results of the information technology security evaluation work performed by TSTC on behalf of the U.S. Environment Protection Agency's Office of Inspector General (OIG). The report includes TSTC's completed Fiscal Year 2007 FISMA Reporting Template, as prescribed by the Office of Management and Budget (OMB).

If you or your staff have any questions or feedback regarding this report, please contact me at (703) 798-6495, tgangi@totalsystech.com or Mark Podracky at (703) 802-4970, mpodracky@totalsystech.com.

Sincerely,

____

Thomas Gangi, TSTC
Project Manager and Senior Auditor

Table of Contents

Chapters

Chapter 1 - Executive Summary

Background

Total Systems Technologies Corporation (TSTC) was tasked to conduct an assessment of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) Federal Information Security Management Act (FISMA) compliance and their progress in meeting the requirements to manage privacy information as described in the OMB Memorandum M-07-19 [FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management]. In performing this evaluation, we reviewed documentation related to prior CSB audits/assessments, security evaluations, security program reviews, reports addressing CSB's information security and privacy program and practices; and conducted an internal and external vulnerability scan of the CSB network. We also reviewed documentation supporting security training, security-related information technology planning efforts, and documentation relevant to CSB information security policies and procedures. It is important to note that OMB issues specific FISMA reporting guidance for agencies comprised of 100 employees or less - which OMB defines as "Micro-agencies" – and that CSB meets the OMB criteria for a micro-agency. Please reference Appendix A for the results of our evaluation consistent with the micro-agencies report format.

Summary of Results

Overall, it is TSTC's conclusion that the CSB Security Program is acceptable. The CSB continues to improve their security posture and has made significant progress in addressing many of the FY 2006 findings. The following table (Table 1) indicates the status of the FY 2006 findings/recommendations.

Table 1: Status of FY 2006 Findings

FY 2006 Finding[1]	Status	Notes
FY06-OIG-IT-01 C&A Process **Issue Summary:** The CSB GSS System Security Plan (SSP) required updating and that, as a whole, the GSS had not been assigned a risk categorization according to the FIPS 199 criteria.	Closed	A review of the CSB GSS Security Plan found that it is consistent with NIST SP 800-18 guidance.
	Closed	A risk categorization has been assigned to the CSB GSS in accordance with FIPS 199 and NIST SP 800-60. However, there are some minor inconsistencies in the roll-up that should be corrected. The overall categorization will not be affected by these corrections.

[1] Please note that the "Issue Summary" sections within this table represent issues identified, and pulled directly from, the FY2006 CSB FISMA Audit Report. They do not represent the current status of these issues. Please refer to the status and notes columns for the current status.

FY 2006 Finding[1]	Status	Notes
	Closed	A test of the CSB GSS security controls occurred. A NIST SP 800-53 based self assessment was performed and documented on 07/10/2007.
FY06-OIG-IT-02 Security Incident Reporting **Issue Summary:** 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	Closed	A review indicated that CSB had developed, and shared with employees during training, procedures for reporting computer security incidents.
FY06-OIG-IT-03 Personally Identifiable Information **Issue Summary:** CSB has not identified or implemented any policies and procedures which explicitly address the protection of sensitive agency information. Existing policies had addressed remote access to PII through Virtual Private Networks and Secure Socket Layer, but does not address PII that is physically removed. POA&Ms should be created for any weaknesses.	Open	A review of the Agency's PII program using the security checklist and guidelines as prescribed by OMB Memorandum 06-16 was in process prior to September 30, 2007, but was not yet completed.
	Closed	A review of the CSB POA&M process did indicate that a POA&M was created, is being managed, and reported for all identified weaknesses.

FY 2006 Finding[1]	Status	Notes
FY06-OIG-IT-04 System Configuration and Patch Management **Issue Summary:** 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 and utilized checklists.	Closed	A review indicated that the CSB did develop and implement an Agency-wide security configuration policy and associated procedures. The CSB has also updated the Patch Management and System Update policy to indicate steps for ensuring newly implemented systems are updated to the latest software versions and tested appropriately. While the CSB test environment is limited (consistent with an organization of its size), CSB is adequately testing before placing patches into production. The CSB has also implemented a policy and procedures to ensure that the IT department is consistent by using a System Setup Checklist to set up new computers. The Checklist does include required security configuration settings.
FY06-OIG-IT-05 Security Control Implementation **Issue Summary:** CSB had not tested its contingency plan during FY 2006. Furthermore, it disclosed that CSB could improve its contingency planning efforts in the areas of: (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. It was also determined that an e-authentication risk assessment was not completed during FY 2006.	Closed	CSB did establish the POA&M item to conduct a test of the CSB GSS contingency plan. .
	Closed	An annual test of the contingency plan of the GSS was successfully performed by CSB on August 31, 2007. Comprehensive backup and recovery procedures were exercised during this test.
	Closed	A review of the CSB Contingency Plan found that it is compliant with NIST SP 800-34 guidance.
	Closed	A review indicated that the CSB had conducted and documented the e-authentication risk assessment.

As the CSB continues to realize improvements in all facets of their information security program, our FY07 evaluation identified several areas that will require continued management focus. The table below (Table 2) summarizes the findings identified during the review.

Table 2 – FY 2007 Findings

FY 2007 Finding	Status	Remarks	Recommendations
FY07-OIG-IT-01 Security Awareness and Training	Open	CSB is conducting and documenting Security Awareness Training for all users of its IT systems. However "specialized" role-based security training needs	1. Expand the security training to include specialized, role-based training in areas specific

FY 2007 Finding	Status	Remarks	Recommendations
		to be improved.	to: security roles / administration; incident response; and contingency planning and implementation. 2. Document the specialized training in a manner similar to that used for the annual user training.
FY07-OIG-IT-02 Policy and Procedures	Open	The CSB has developed Incident Response policies and procedures and integrated them within their security training. Although the policies and procedures exist, there is little supporting evidence that these would work or be effective.	3. Annual testing, at a minimum, should be done to verify the Incident Response Procedures. A documented "Table Top" test, using a privacy data (PII) breach scenario, would address security incidence response as well as of PII incidents as mandated by OMB
FY07-OIG-IT-03 Personally Identifiable Information	Open	Agencies are required by OMB memorandum (M-07-16) of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" to develop and implement a breach notification policy within 120 days. Although development of this policy was in process, as of September 30, 2007, CSB had not yet completed the Breach Policy.	4. Understand and document the Breach Policy requirements and finalize a policy that meets CSB needs and OMB requirements 5. On an annual basis, test the policies and procedures for effectiveness.
FY07-OIG-IT-04 Configuration Management	Open	On occasion, it is necessary for CSB to implement system configuration changes that may result in systems having non-standard security configurations.	6. Update the security policy and associated procedures to address reviewing, approving and documenting non-standard security configurations
FY07-OIG-IT-05 Security Program Management	Open	There is uncertainty by CSB Management as to what needs to be reported to OMB regarding the POA&M.	7. On an annual and/or semi-annual basis, communicate and coordinate with OMB to gain consensus on the CSB FISMA

FY 2007 Finding	Status	Remarks	Recommendations
			Reporting requirements.
	Open	The roles and responsibilities of the CSB ITSO are identified in Board Order 034 but evidence of the acknowledgement of those roles and responsibilities was not available.	8. CSB should draft and place on file a signed acknowledgment letter depicting the roles and responsibilities of the CSB ITSO.
FY07-OIG-IT-06 C&A Process	Open	CSB has performed the FIPS 199 categorization for its GSS but there are inconsistencies with the roll-up of the various elements of that categorization. In conclusion, while the plan overall was categorized in accordance with FIPS 199, sub elements of the categorization were done in error. This did not impact the overall categorization of moderate that CSB had arrived at, and as a result the categorization will remain moderate	9. CSB should follow a documented standard for accessing various FIPS 199 elements to avoid any inconsistencies.
	Open	Effective October 1, 2006, security control requirements changed from NIST SP 800-26 to the NIST SP 800-53 requirements. These control requirements form the basis for the C&A Artifacts.	Leveraging samples/templates from other Agencies, begin to update applicable: 10. System Security Plan(s) 11. Risk Assessment(s) 12. Security Test Procedures, and Security Assessment Results to address the NIST SP 800-53 controls. It is further recommended that these documents be updated to coincide with the annual 1/3 testing requirement of the NIST SP 800-53 controls.
FY07-OIG-IT-07 Security Control Procedures	Open	The NIST SP 800-53 Self Assessment does not correctly or consistently reflect that the controls were tested. In reviewing the tested controls we found that CBS security had not "marked" the tested controls column to indicate the control(s) as tested.	13. Mark the "tested" column for the controls that were tested and provide details of the test and its results in the "description / remarks" field.

Chapter 2 - Evaluation Results

Assessment Area 1 - FISMA Systems Inventory

Evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized), identify the number of agency and contractor systems, and the number of systems reviewed. Extend the worksheet onto subsequent pages if necessary to include all components/bureaus.

The Chemical Safety Board (CSB) inventory consists of one general support system (GSS). While CSB has performed the FIPS 199 categorization for this GSS, there are three inconsistencies with the roll-up of the various elements of that categorization that do not impact the overall categorization of "moderate**".** For example, the GSS system security plan (SSP) document indicates an overall categorization of MEDIUM – while three elements of subsystems making up the overall GSS within this categorization are indicated as HIGH**.** This contradicts guidance which states that if any elements are determined to be HIGH, then an overall categorization of HIGH is required**.** Upon further discussion with CSB security staff it was indicated that these three elements should have been recorded as "medium" and these changes will be recorded in the FY08 annual update of the SSP.

Recommendation

CSB should

- Follow a documented standard for accessing various FIPS 199 elements to avoid any inconsistencies.

Assessment Area 2 - C&A, Security Controls Testing, and Contingency Plan Testing

Identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

Security Category	Total Number	Total Percent
Number and percentage of systems certified and accredited	1	100%
Number and percentage of systems where security controls are tested	1	100%
Number and percentage of systems with tested contingency plans in accordance with policy	1	100%

Although an assessment was performed in support of the C&A process, the NIST SP 800-53 Self Assessment does not correctly reflect that the security controls were actually tested.

CSB should:

- Mark the "tested" column for the controls that were tested and provide details of the test and its results in the "description / remarks" field

Assessment Area 3 - Oversight of Contractor Systems

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.

CSB currently tracks its IT inventory using commercial off-the-shelf database/worksheets. The database is updated at least annually or when the CSB security staff determines that changes/deletions are needed. Please reference the table below for a status of the individual OMB criteria.

OMB FY2007 Evaluation Metric	Result
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.	N/A – No CSB systems are currently owned or operated by a contractor.
The agency has developed a complete 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. [2]	The inventory is approximately 96-100% complete. The CSB maintains a complete list of all systems. CSB has no national security systems.
The IG generally agrees with the CIO on the number of agency-owned systems.	Yes. The EPA OIG agrees with the CIO concerning the number of information systems.
The IG 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 agrees that no information systems are used or operated by contactors.
The agency inventory is maintained and updated at least annually.	Yes. The CSB inventory is maintained and updated at least annually

[2] Per OMB FY2007 FISMA Guidance, the metrics used in assessing this requirement include:
- The inventory is approximately 0-50% complete
- The inventory is approximately 51-70% complete
- The inventory is approximately 71-80% complete
- The inventory is approximately 81-95% complete
- The inventory is approximately 96-100% complete

OMB FY2007 Evaluation Metric	Result
If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.	N/A. The CSB inventory is 96-100% complete.

Assessment Area 4 - Plan of Action and Milestones (POA&M) Process

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

The CSB has a POA&M process in place and they are almost always (96-100% of the time) proactively developing, managing, and prioritizing their POA&Ms in accordance with guidelines. Control weaknesses from prior audits / reviews are routinely reviewed and reconciled. However, CSB Management does not have clear guidance on the required OMB FISMA reporting standard which is causing an uncertainty / inconsistency of the required content and submission format associated with the OMB FISMA reporting.

Recommendation

CSB should:

- On an annual and/or semi-annual basis, communicate and coordinate with OMB to gain consensus on the CSB FISMA Reporting requirements. While quarterly reporting is not currently a micro-agency requirement, the CSB should be reviewing the POA&M and collecting/documenting supporting evidence and be prepared to report on a quarterly basis, if requested.

OMB FY2007 Criteria[3]	Result
The POA&M is an agency-wide process, incorporating all known information technology 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.	Almost Always: 96-100% of the time.
When an information technology 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).	Almost Always: 96-100% of the time.
Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always: 96-100% of the time.
Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a	Almost Always: 96-100% of

[3] OMB FY2007 FISMA Guidance describes the response categories as follows:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

OMB FY2007 Criteria[3]	Result
quarterly basis.	the time.
IG/external audit findings are incorporated into the POA&M process.	Almost Always: 96-100% of the time.
POA&M process prioritizes information technology security weaknesses to help ensure significant information technology security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always: 96-100% of the time.

Assessment Area 5 - Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

OMB C&A Process Rating Scale	IG Rating of CSB FY2007 C&A Process
Excellent	
Good	X
Satisfactory	
Poor	
Failing	

The CSB IG's quality rating included (or considered) the following aspects of the CSB C&A process	
System Security Plan	X
System impact level	X
System test and evaluation	
Security control testing	X
Incident handling	X
Security awareness training	X
Security configurations (including patch management)	X

During our review of the CSB C&A process, we obtained the C&A package for the CSB GSS – and the associated security artifacts (SSP, POA&M, etc.). Our review of the GSS documentation showed consistent adherence with federal requirements, however the roles and responsibilities of the CSB ISO, although defined in Board Order 034, does not appear to be formally acknowledged in writing by the ITSO.

The CSB has tested the security controls consistent with the change from NIST SP 800-26 to the NIST SP 800-53 requirements In evolving its security program, CSB needs to incorporate these control changes into its security documentation so that there is a consistency between control requirements (NIST SP 800-53), implemented control descriptions (SSP), and control testing procedures and results. Also, OMB now requires that 1/3 of the controls be tested annually. As stated in the Area 2 discussion, the NIST SP 800-53 Self Assessment does not consistently or correctly reflect that the controls were actually tested with a description of the tests performed and the actual results.

Recommendation

CSB should:

- Draft and place on file an acknowledgment letter depicting the accepted roles and responsibilities of the CSB ITSO.

- Leveraging samples/templates from other Agencies, begin to update:

    - System Security Plan
    - Risk Assessments
    - Security Test Procedures, and Security Assessment Results

    to address the NIST SP 800-53 controls. It is also recommended that these documents are updated to coincide with the annual requirement regarding the testing of 1/3 of the NIST SP 800-53 controls (continuous monitoring requirement from OMB).

Assessment Area 6 - Privacy Impact Assessment (PIA) Process

Provide a qualitative assessment of the agency's PIA process, including adherence to existing policy, guidance, and standards.

OMB Process Rating Scale	IG Rating of CSB FY2007 PIA Process
Excellent	
Good	
Satisfactory	
Poor	
Failing	

We determined during our evaluation that the CSB review of their PII program using the security checklist and guidelines, as prescribed by OMB Memorandum 06-16, was not completed prior to September 30, 2007. However, our evaluation did indicate that significant progress has been made in this area as of that date. Upon completion of this activity, the PIA process would ascend to a rating of "Good".

Assessment Area 7 - Configuration Management

Approximate the extent to which applicable systems implement common security configurations established by NIST.

During our FY2007 evaluation we determined that CSB had developed a comprehensive configuration policy and now has a formal policy that mandates the use of a Computer Setup Checklist for all new computer installations – specifying the CSB security configuration settings. Our vulnerability test results concluded that CSB is also mitigating vulnerabilities through its configuration and patch management processes. However, we found that, on occasion, it is necessary for CSB to implement system configuration changes that may result in the systems having non-standard security configurations. An example we found was the following: for remote users (laptops) it may be necessary to grant administrative privileges so that when they are offsite and need to be able to change remote/network connectivity settings they can. This allows the remote users to continue to communicate with CSB. This deviation from the standard configuration needs to be documented and approved prior to it being implemented.

A formal process of requesting, approving, and documenting these exceptions/waivers was not in place.

Recommendation

CSB should:

- Update the security policy and associated procedures to address reviewing, approving, and documenting non-standard security configurations

Assessment Area 8 - Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement.

OMB FY2007 FISMA Guidance	Result
The agency follows documented policies and procedures for identifying and reporting incidents internally.	**YES**
The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).	**YES**
The agency follows documented policies and procedures for reporting to law enforcement authorities.	**YES**

The CSB has developed incident response policies and procedures and integrated them within their security training. Although the policies and procedures exist, there is little supporting evidence that these would work or be effective since these have not been formally tested and a security incident did not occur in FY07.

Recommendation

CSB should:

- Conduct annual testing to verify and update, as required, the incident response procedures. A documented "Table Top" test, using a privacy data (PII) breach scenario, would address security incidence response as well as of PII incidents as mandated by OMB.

Assessment Area 9 - Security Awareness Training

The agency has ensured security awareness training of all employees, including contractors and those employees with significant information technology security responsibilities.

We determined that all CSB employees and contractors had received the appropriate end user security awareness training and the appropriate level of supporting documentation had been maintained. The CSB is conducting and documenting annual Security Awareness Training for all users of its IT systems. However, in support of NIST SP 800-53 Control requirements for moderate categorized systems, "specialized," role-based security training could be improved.

Recommendation

CSB should:

- Build upon the current security training to include specialized, role-based training in areas specific to: security roles/administration; incident response; and contingency planning and implementation. This training is for staff that is in those specialized roles.

- Document the specialized training in a manner similar to that used for the annual user security training.

Assessment Area 10 - Peer-to-Peer File Sharing

The agency explain policies regarding peer-to-peer file sharing in information technology security awareness training, ethics training, or any other agency-wide training.

During the FY2007 review we verified that CSB personnel had completed the annual security training that included policies and procedures relevant to peer-to-peer file sharing. Furthermore, peer-to-peer file sharing is not supported or condoned at the CSB and the configurations we examined did not have peer-to-peer file sharing software installed or configured.

Assessment Area 11 - E-authentication Risk Assessments

The agency has completed system e-authentication risk assessments.

During our FY2007 evaluation, we determined that an E-authentication Risk Assessment was completed. The CSB could enhance the assessment by strengthening the underlying documentation used to support the assessment.

Safeguarding Against and Responding to the Breach of PII

Agencies are required by OMB memorandum (M-07-16) of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" to develop and implement a breach notification policy within 120 days.

Although development of this policy was in process, as of September 30, 2007, CSB had not yet completed the Breach Policy as described in OMB Memorandum M-07-16.

Recommendation

CSB should:

- Become familiar with the requirements identified in OMB Memorandum M-07-16, document the Breach Policy requirements, and finalize the policy that meets CSB needs and OMB requirements.[4]

- On an annual basis, test the Breach of PII policies and procedures for effectiveness.

[4] These requirements include: the drafting of a breach notification policy; drafting of an implementation plan to eliminate unnecessary use of Social Security Numbers; drafting of an implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII); and, drafting of a policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow the rules.

Appendix A - Micro Agency Reporting Template

Microagency Reporting Template for FY 2007 FISMA and Information Privacy Management

Agency Name:	Chemical Safety and Hazard Investigation Board (CSB)
Agency Point of Contact:	Anna Johnson, CIO, CSB

Microagencies are defined as agencies employing 100 or fewer Full Time Equivalent positions (FTEs). Microagencies must report to OMB annually on FIMSA and Information Privacy Management. While quarterly reports/updates are not required, microagencies should be prepared to provide information or to begin submitting quarterly reports to OMB upon request.

1. Information Systems Security

a.	Total Number of agency and contractor systems	1
b.	Number of agency and contractor systems certified and accredited	1
c.	Number of agency and contractor systems for which security controls have been tested and reviewed in the past year	1
d.	Was an independent assessment conducted in the last year?	Yes
e.	Number of employees and contractors	42
f.	Number of employees and contractors who received IT security awareness training in the last year	42

2. Information Privacy

a. **Breach Notification**
Agencies are required by OMB memorandum (M-07-16) of May 22, 2007, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” to develop and implement a breach notification policy within 120 days.

Please certify whether your agency has completed the requirements of M-07-16 by answering "Yes" or "No" to questions (1) through (4) in the table below.

I certify the agency has completed:		
1.	A breach notification policy (Attachment 3 of M-07-16)	No
2.	An implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1 of M-07-16)	No
3.	An implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1 of M-07-16)	No
4.	Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 4 of M-07-16)	No

Note: Micro agencies must maintain all documentation supporting this certification, and make it available in a timely manner upon request by OMB or other oversight authorities. **Micro Agencies are not required to provide the actual documentation with the annual report.**

Microagency Reporting Template for FY 2007 FISMA and Information Privacy Management

Agency Name:	Chemical Safety and Hazard Investigation Board (CSB)
Agency Point of Contact:	Anna Johnson, CIO, CSB

b. **Privacy Impact Assessments (PIAs) and Systems of Record Notices (SORNs)**
Please provide the URL to a centrally located web page on the agency web site on which the agency lists working links to all of its PIAs and working links to all of its SORNs published in the Federal Register. Agencies must maintain all documentation supporting this certification and make it available in a timely manner upon request by OMB or other oversight authorities. By submitting the template the agency certifies that to the best of agency's knowledge the quarterly report accounts for all of the agency's systems to which the privacy requirements of the E-Government Act and Privacy Act are applicable. If the agency does not have any PIAs or SORNS, enter "NA."

b.1.	Provide the URL of the centrally located page on the agency web site listing working links to agency PIAs: (Hyperlink not required)	N/A
b.2.	Provide the URL of the centrally located page on the agency web site listing working links to the published SORNs: (Hyperlink not required)	www.csb.gov/index.cfm?folder=legal_affairs&page=index

Appendix B - CSB's Response to Draft Report

March 25, 2008

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

Dear Mr. Brevard:

We have reviewed the draft report on 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 completing actions on FISMA findings from Fiscal Year (FY) 2006. While the draft report shows 9 of 11 findings are closed, we believe the report should show that 10 of the 11 findings are closed. Finding FY06-OIG-IT-01 should be considered closed because the CSB completed all the recommendations for this finding in FY 2007, including assigning an overall risk categorization. The FY 2007 FISMA evaluation found some inconsistencies in the roll-up (Finding FY07-OIG-IT-06) that the CSB will correct this year. Showing the FY 2006 Finding as open in the draft report will double count the one FY 2007 Finding.

We agree that FY06-OIG-IT-03 should be considered open. The CSB was reviewing its personally identifiable information (PII) program in FY 2007, but did not complete the review and related work in FY 2007. In FY 2008 we have developed a comprehensive Board Order on PII, and expect that this will go to the full Board for approval by April 30, 2008.

We also agree with the FY 2007 findings summarized in Table 2 of the draft report. 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 is submitted to the Office of Management and Budget, 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,

John S. Bresland
Chairperson

Enclosure

FY 2007 FISMA Finding	Status	Planned Actions
FY07-OIG-IT-01 Security Awareness and Training	Open	**<u>By May 31, 2008, the CSB will</u>:** 1. Expand the security training to include specialized, role-based training in areas specific to: security roles/administration; incident response; and contingency planning and implementation. 2. Document the specialized training in a manner similar to that used for the annual user training.
FY07-OIG-IT-02 Policy and Procedures	Open	**<u>By May 15, 2008, the CSB will</u>:** 3. Conduct the first annual test to verify the Incident Response Procedures. A documented "Table Top" test, using a privacy data (PII) breach scenario, will be used to address security incidence response as well as of PII incidents as mandated by OMB.
FY07-OIG-IT-03 Personally Identifiable Information	Open	4. The CSB has documented the Breach Policy requirements and finalized a policy that meets CSB needs and OMB requirements. (Board Order 034, Appendix J, approved by the Board December 5, 2007.) **<u>By May 15, 2008 the CSB will</u>:** 5. Conduct the first annual test of breach policies and procedures for effectiveness.
FY07-OIG-IT-04 Configuration Management	Open	**<u>By September 30, 2008, the CSB will</u>:** 6. Update the security configuration policy and associated procedures to address reviewing, approving and documenting non-standard security configurations.
FY07-OIG-IT-05 Security Program Management	Open	**<u>By March 31, 2008, the CSB will</u>:** 7. Communicate and coordinate with OMB to gain consensus on the CSB FISMA Reporting requirements, and will communicate with OMB on at least an annual basis. 8. Draft and place on file a signed acknowledgment letter depicting the roles and responsibilities of the CSB ITSO.

FY 2007 FISMA Finding	Status	Planned Actions
FY07-OIG-IT-06 C&A Process	Open	**By August 31, 2008, the CSB will:** 9. Follow a documented standard for accessing various FIPS 199 elements to avoid any inconsistencies.
	Open	**By August 31, 2008, the CSB will:** Update the following to address the NIST SP 800-53 controls: 10. System Security Plan(s) 11. Risk Assessment(s) 12. Security Test Procedures, and Security Assessment Results Updates will coincide with the annual 1/3 testing requirement of the NIST SP 800-53 controls.
FY07-OIG-IT-07 Security Control Procedures	Open	**By July 31, 2008, the CSB will:** 13. Test security controls and mark the “tested” column for the controls that were tested and provide details of the test and its results in the “description / remarks” field.