U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2008)

Report No. 08-P-0295

September 29, 2008

U.S. Environmental Protection Agency
Office of Inspector General

08-P-0295
September 29, 2008

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 of 2002 (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 2008 FISMA assessment under the direction of the U.S. Environmental Protection Agency (EPA) Office of the Inspector General (OIG). The review adhered to the Office of Management and Budget (OMB) 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/2008/20080929-08-P-0295.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 2008)

What TSTC Found

During Fiscal Year 2008, CSB continued to make significant progress in improving the security of its information system resources. CSB had done this by performing the following:

- Expanding the security training to include specialized, role-based training;
- Implementing incident response training and testing and issuing a Breach Policy; and
- Benchmarking and utilizing government and industry best practices and templates in updating the CSB Certification and Accreditation documentation, including the System Security Plan, the Risk Assessment, and the security test controls.

CSB has also taken the steps necessary to allow CSB management to align the organization's security program with the Personally Identifiable Information requirements issued by the OMB. CSB also took the necessary steps to complete six of the seven planned actions in response to the security weaknesses identified during the Fiscal Year 2007 audit. The remaining weakness regarding non-standard security configurations from the Fiscal Year 2007 audit is on schedule to meet the target completion date of October 10, 2008.

What TSTC Recommends

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

- Insert the approved security "banner" within all CSB database applications.
- Continue to update the CSB Configuration Management policy and associated procedures to address reviewing, approving, and documenting non-standard security configurations to meet the deadline established by CSB.
- Continue to update, as applicable, the appropriate security documentation to ensure compliance with National Institute of Standards and Technology Special Publication 800-53 controls guidance and update the security documents to include revision history information such as date of revision, individual who updated the document, and description of the revision.

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

OFFICE OF
INSPECTOR GENERAL

September 29, 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 2008)
Report No. 08-P-0295

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

TO: The Honorable John S. Bresland
Chairperson
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 $6,224. This cost does not include the contracting service cost, 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.

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 2008)

September 29, 2008

REPORT CONTRIBUTORS

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

ABBREVIATIONS

ATO	Authority to Operate
AITSO	Assistant Information Technology Security Officer
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
IT	Information Technology
ITSO	Information technology Security Officer
LAN	Local Area Network
MIS	Management Information 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
RA	Risk Assessment
SP	Special Publication
SSL	Secure Socket Layer
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

September 29, 2008

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 2008 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. Environmental Protection Agency's Office of the Inspector General (OIG). The report includes the TSTC completed Fiscal Year 2008 FISMA Reporting Template, as prescribed by the Office of Management and Budget (OMB), the completed CSB microagency template and the CSB response to the findings depicted within this report.

If you or your staff have any questions or feedback regarding this report, please contact me at (703) 802-4970, 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-08-21 -*FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. In performing this evaluation, TSTC 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. TSTC also reviewed documentation supporting security training and documentation relevant to CSB information security policies and procedures. The analysis also involved interview sessions with CSB IT security staff**.**

Summary of Results

Overall, it is the conclusion of TSTC that the CSB Security Program has a rating of GOOD. The CSB continues to improve their security posture and has made significant progress in addressing the majority of the FY 2007 findings. The following table (Table 1) indicates the status of the FY 2007 findings and recommendations.

Table 1: Status of FY 2007 Findings

FY 2007 Finding	Status	Notes
FY07-OIG-IT-01 Security Awareness and Training **Issue Summary:** CSB should expand the security training to include specialized, role-based training in areas specific to: security roles / administration; incident response; and contingency planning and implementation. They should also document the specialized training in a manner similar to that used for the annual user training.	Closed	We conducted a review of the CSB security awareness training materials, rosters and training acknowledgment forms. We also interviewed CSB IT security staff to gain an understanding of the training environment. The CSB IT staff has developed and implemented specialized IT training. A review of the materials indicates that those performing security roles understand, and have been trained in, their roles. CSB is also maintaining signed "Roles" acknowledgement forms for those (ITSO and AITSO) performing these security duties.

FY 2007 Finding	Status	Notes
FY07-OIG-IT-02 Policy and Procedures **Issue Summary:** CSB should conduct annual testing, at a minimum, 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.	Closed	We conducted a review of the CSB incident response policy document and interviewed CSB security staff. During the fiscal year (05/14/2008), CSB tested the incident response procedures by testing two scenarios: 1. A data "breach" scenario, and, 2. a lost laptop scenario. The testing plan and results were documented and led by the ITSO and AITSO. The documentation was sufficient.
FY07-OIG-IT-03 Personally Identifiable Information **Issue Summary:** CSB should document the Breach Policy requirements and finalize a policy that meets CSB needs and OMB requirements. Also, on an annual basis, CSB should test the policies and procedures for effectiveness.	Closed	We conducted a review of the CSB breach policy and procedures documentation and interviewed CSB security staff. The CSB has finalized the policy and tested the procedures (05/14/2008) during their incident response testing indicated in FY07-OIG-IT-02 above. The procedures, as currently in place, are effective.
FY07-OIG-IT-04 Configuration Management **Issue Summary:** CSB should update the security policy and associated procedures to address reviewing, approving and documenting non-standard security configurations**.**	Open	This finding is still open. According to the CSB response to this FY2007 finding, the target completion date is 09/30/2008. As of the compilation of this report, the deadline date is still in the future. During the interview with the CSB IT security staff, it was indicated that this effort is in progress. As a result of the timing of this report and the current ongoing work, the finding will be reported as open.

FY 2007 Finding	Status	Notes
FY07-OIG-IT-05 Security Program Management **Issue Summary:** On an annual and/or semi-annual basis, CSB should coordinate with OMB to gain consensus on the CSB FISMA reporting requirements. CSB should also draft - and place on file - a signed acknowledgment letter depicting the roles and responsibilities of the CSB ITSO.	Closed	We conducted a review of the CSB communications (emails) disseminated to OMB and interviewed CSB security staff. The CSB security staff has attempted numerous and methodical communications with OMB seeking guidance and clarity regarding specific FISMA reporting requirements. We also reviewed the on-file acknowledgment letter depicting the roles and responsibilities of the CSB ITSO. The acknowledgement letter is concise and clearly indicates the roles/responsibilities of the CSB ITSO and AITSO.
FY07-OIG-IT-06 C&A Process **Issue Summary:** CSB should follow a documented standard for accessing various FIPS 199 elements to avoid any inconsistencies. Also, leveraging samples/templates from other Agencies, CSB should update the System Security Plan; the Risk Assessment; and, the Security Test Procedures/ Results.	Closed	We conducted a comprehensive review of the CSB C&A process. This review included analysis of the CSB GSS FIPS 199, System Security Plan; the Risk Assessment; and, the Security Test Procedures/ Results documentation. The analysis also involved interviews with the CSB security staff. The CSB security staff is actively leveraging available templates and their documentation is consistent with current NIST guidance.
FY07-OIG-IT-07 Security Control Procedures **Issue Summary:** The CSB security staff should update the test controls artifact by marking the "tested" column for the controls that were tested and provide details of the test and its results in the "description / remarks" field.	Closed	We conducted a comprehensive review of the CSB test controls documentation. The document is consistent with NIST guidance and test results (and status) are properly indicated within the documentation.

Although CSB continues to realize improvements in all facets of their information security program, our FY2008 evaluation identified several areas that will require continued IT security management focus. The following table (Table 2) summarizes the findings identified during the review. Note that all of these findings are considered low risk.

Table 2 – FY 2008 Findings

FY 2008 Finding	Status	Remarks	Recommendations
FY08-OIG-IT-01 Security Controls Testing	Open	NIST guidance recommends testing - at a minimum - one third of the system controls each FY. This is to ensure that over the course of a three-year cycle – all security controls are tested and updated.	CSB should continue to update, as applicable, the appropriate security documentation to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls guidance. Develop a plan to ensure that the CSB IT security staff is testing approximately one-third of unique security controls per year and an Agency-defined set of key controls every year. Any vulnerabilities identified as a result of this testing should be tracked in the CSB POA&M.
FY08-OIG-IT-02 C&A Process	Open	The C&A documents (SSP, FIPS 199, RA, CP, Test documents, etc.) do not currently include revision dates and history of changes.	CSB should update the current C&A documentation to include revision history information such as date of revision, individual that updated the document, and description of the revision. This should be a standard practice going forward to ensure the latest version(s) of documents is in place.
FY08-OIG-IT-03 Privacy Impact and Management	Open	While users accessing the CSB GSS are presented with a banner indicating the system is a government system and therefore protected, the individual database application systems located within the GSS do not display the banner.	CSB IT staff should insert the approved banner so that it is presented to all users accessing individual databases within CSB. This is especially important for the "Investigations" system, because that system has the potential to contain Personally Identifiable Information (PII).
FY08-OIG-IT-04 Configuration Management	Open	This finding was initially documented during the FY07 audit. The Configuration Management Plan does not contain sufficient detail to indicate non-standard security configurations. **[**	CSB should continue to focus on and update the security policy and associated procedures to address reviewing, approving and documenting non-standard security configurations to meet the CSB designated target completion date of 09/30/2008.

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 still consists of a single general support system (GSS). This GSS is essentially composed of their MIS LAN, web site and local telecommunications infrastructure. A review of the FIPS 199 categorization for the GSS showed that the inconsistencies identified in last year's (FY 2007) assessment have been corrected and the IT security staff has correctly categorized the system as Moderate. The IT inventory is currently maintained and up-to-date. The CSB utilizes a Microsoft Access™ database (the "Inventory Management System") for storing and managing IT inventory information. The system also allows CSB IT security staff to track ownership of IT assets down to the user level and obsolete inventory is also tracked within the system. The system also allows the CSB IT staff to produce a number of reports – this functionality was observed during the interview portion of this assessment. Information within the FIPS 199 is also consistent with the information indicated within the CSB GSS System Security Plan (SSP).

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%

A comprehensive review of the CSB SSP and security controls and test results indicates that CSB is proactively managing the CSB IT infrastructure. Currently, CSB maintains only one system requiring a C&A – the CSB General Support System (GSS). The test controls indicated within the security controls self-assessment that map to the CSB GSS are consistent with those indicated within the CSB SSP. In addition, CSB IT security staff have revisited the test controls status and updated them accordingly to reflect the fact that they have been tested. These actions close a finding identified during the FY2007 assessment. Care must be taken to ensure that the CSB IT security staff is testing approximately one-third of the security controls per year. This

will allow them to meet guidance which suggests testing controls at a pace that sufficiently ensures all controls are tested in any given 3-year period.

Recommendation

CSB should:

FY08-OIG-IT-01

Develop a plan to ensure that the CSB IT security staff is testing approximately one-third of the required NIST SP 800-53 security controls per year (based upon a FIPS 199 categorization of "moderate") and a set of CSB-defined key controls annually. This will allow CSB to meet guidance which suggests testing controls at a pace that sufficiently ensures all controls are tested in any given 3-year period.

Assessment Area 3 - Oversight of Contractor Systems and Quality of Agency System Inventory

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.

A review of the CSB IT system inventory and interviews with CSB IT security staff indicates that the CSB maintains no contractor-operated systems. CSB currently tracks its IT inventory using a Microsoft Access database developed with Microsoft SQL code. The database is updated as changes in inventory warrant and a review of the database indicates that the CSB IT security staff accurately maintains the inventory. Please reference the table below for a status of the individual OMB criteria.

OMB FY2008 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. [1]	The inventory is approximately 96-100% complete. The CSB maintains a complete list of all systems. CSB has no national security systems.

[1] Per OMB FY2008 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

OMB FY2008 Evaluation Metric	Result
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
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 – Evaluation of 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 (utilizing the Microsoft Office products Word and Excel) and the CSB is almost always (96-100% of the time) proactively developing, managing, and prioritizing their POA&Ms in accordance with guidelines. A review of the POA&M process artifacts and quarterly reports, along with interviews with CSB IT security staff indicates that control weaknesses from prior audits / reviews are routinely reviewed and reconciled. Last year's (FY 2007) assessment indicated that CSB Management should coordinate and communicate with OMB more closely to determine OMB FISMA reporting standards. A review of correspondence (email) between CSB and OMB indicates that the CSB has repeatedly reached out to OMB. Please reference the following table for a summary of the CSB POA&M process status.

- The inventory is approximately 81-95% complete
- The inventory is approximately 96-100% complete

OMB FY2008 Criteria[2]	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 the CIO 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 quarterly basis.	Almost Always: 96-100% of 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 – Assessment of 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 FY2008 C&A Process
Excellent	
Good	**X**
Satisfactory	
Poor	
Failing	

[2] OMB FY2008 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

The 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	**X**
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, TSTC obtained the current C&A package for the CSB GSS – and the associated security artifacts (SSP, RA, POA&M, etc.). Our review of the GSS documentation showed that CSB is making better use of C&A templates available to Federal Agencies – utilizing those consistent with federal requirements. In addition, the CSB IT security staff developed Roles and Responsibilities documents necessary to clearly indicate the responsibilities of both the ITSO and AITSO. This mitigates a finding identified during last year's (FY 2007) assessment. The C&A documents are current and periodically updated, however, the documentation should be updated to include revision history (date last updated, by whom, reason for revision, etc.) to ensure version control and that the latest versions of these documents are in place.

Recommendation

CSB should:

FY08-OIG-IT-02

Update the current C&A documentation to include revision history information such as date of revision, individual that updated the document, and description of the revision the latest revision dates, the person(s) making the revisions and the reason for the revision. This should be a standard practice going forward to ensure the latest version(s) of documents are in place.

Assessment Area 6 – Assessment of 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 FY2008 PIA Process
Excellent	
Good	**X**
Satisfactory	
Poor	
Failing	

A review of the CSB documentation, and interviews with CSB IT security staff, indicates that CSB has conducted a review of their PII program using the security checklist and guidelines, as prescribed by OMB Memorandum 06-16.

In addition, during a review of CSB systems and in interviews with CSB IT security staff, the CSB does not currently provide any system access to the general public (aside from their public facing web site), or any public-facing systems access requiring userids / passwords. Specifically, the only public facing site they have is the CSB web site, and it does not require a login and does not interface with internal systems or contain PII – thus not requiring a publicly posted PIA.

During our interview with CSB IT security staff, we also observed the "Investigations" system. Although PII is not currently present, the potential for this system containing PII exists (as a result of PII that may be on imaged supporting documents within the system). Although not a system of record for this PII, privacy policy rules apply to the system. A separate "banner", distinct from the CSB standard system banner, should be inserted to warn prospective users of the "privacy" data that may be contained within the system.

Recommendation

CSB should:

FY08-OIG-IT-03

Insert the approved banner so that it is presented to all users accessing individual databases within CSB. This is especially important for the "Investigations" system, because that system has the potential to contain Personally Identifiable Information (PII).

Assessment Area 7 – Progress of Agency Privacy Program

Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

OMB Progress Rating Scale	IG Rating of CSB FY2008 Privacy Program Progress
Excellent	
Good	**X**
Satisfactory	
Poor	
Failing	

In conducting interviews with CSB IT security staff and reviewing the Breach and Privacy Policies, the vulnerability scan output, and the CSB security and awareness training documents (and logs), the CSB program is operating in a manner consistent with industry and Federal standards – the CSB processes are consistent with OMB and NIST guidance for ensuring PII is protected. The CSB IT security staff also designed, reviewed, and documented a test of their incident response process – using a "breach" scenario as one of the tests. CSB is adequately implementing the provisions of M-07-16.

Assessment Area 8 - Configuration Management

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

During the assessment, TSTC reviewed the scan outputs (internal performed on 08/20/2008 and external performed on 08/27/2008) for the existence of standard configurations and any known vulnerabilities. A review of the inventory database and logs also demonstrated compliance regarding maintaining up-to-date records and documentation. The scans did reveal that two of the CSB mail servers do not have installed a Microsoft Exchange security update. However, the CSB IT security staff was aware of the update, made a decision not to apply it based upon research, and assumed the risk of not currently installing the update since the update has the potential to prevent the MS Exchange store from mounting after a system restart, thus making the e-mail system unavailable.

Although initially documented during the FY07 audit, CSB should continue to address reviewing, approving and documenting non-standard security configurations**.** It is listed here again because this is an on-going process requiring attention to ensure that the confidentiality, integrity and availability of CSB systems are maintained.

Recommendation

CSB should:

FY08-OIG-IT-04

Update the security policy and associated procedures to address reviewing, approving and documenting non-standard security configurations to meet the CSB designated target completion date of 09/30/2008.

Assessment Area 9 - 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 FY2008 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 addressed these within their annual security training. A review of the CSB IT security documentation and interviews indicate that the CSB conducted incident response testing using a "breach" scenario and a lost laptop scenario. Reviews of the Breach and Privacy Policies, the vulnerability scan outputs, and incident response tests processes (and results) indicate a program consistent with industry and Federal standards – and are consistent with NIST guidance. It should be noted that the testing included processes for reporting to both US-CERT and other designated law enforcement officials and organizations.

Assessment Area 10 - 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 reviewed the CSB Annual Security Awareness Training documents and the training rosters (logs) maintained by the CSB IT security staff, as well as the training acknowledgement forms of the CSB security awareness training attendees. All CSB personnel and contractors had received the mandatory FY2008 security awareness training; and the material utilized during the training was comprehensive, up-to-date, and accurate.

Assessment Area 11 – Collaborative Web Technologies and Peer-to-Peer File Sharing

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

During the FY2008 review, we verified that CSB personnel had completed the annual security training that included policies (*i.e.*, the Board 34 document) 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 12 - E-authentication Risk Assessments

The agency has completed system e-authentication risk assessments.

During our FY2008 evaluation, TSTC determined that an E-authentication Risk Assessment was completed. During a review of CSB systems and in interviews with CSB IT security staff, the CSB does not currently provide any system access to the general public (aside from their public facing web site), or any public-facing systems access requiring userids / passwords. Specifically, the only public facing site they have is their web site and it does not require a login and does not interface with internal systems. As a result, no general public userids and/or passwords are maintained by the CSB systems.

Appendix A - Micro Agency Reporting Template

Microagency Reporting Template for FY 2008 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	38
f.	Number of contractors	5
f.	Number of employees and contractors who received IT security awareness training in the last year	43

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)	Yes
2.	An implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1 of M-07-16)	No[3]
3.	An implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1 of M-07-16)	Yes
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)	Yes

[3] The CSB does not have a written plan to eliminate social security numbers from their system although currently no social security numbers are contained within their systems. They will develop the required plan and have a target completion date of November 22, 2008.

Microagency Reporting Template for FY 2008 FISMA and Information Privacy Management	
Agency Name:	Chemical Safety and Hazard Investigation Board (CSB)
Agency Point of Contact:	Anna Johnson, CIO, CSB

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.**

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

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

John S. Bresland
Chairman and CEO

Gary L. Visscher
Board Member

William B. Wark
Board Member

William E. Wright
Board Member

September 26, 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 significant progress in completing actions on FISMA findings from Fiscal Year (FY) 2007. The CSB took the necessary steps to close six of the seven findings, and the seventh, FY07-OIG-IT-04, is on schedule to meet a target completion date of October 10, 2008. This action will also satisfy the requirements to close one of the FY2008 findings, FY08-OIG-IT-04, to address reviewing, approving, and documenting non-standard security configurations.

We also agree with the FY 2008 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
Chairman & CEO

Enclosure

Enclosure

Summary of FY 2008 Findings & CSB Planned Actions

FY 2008 FISMA Finding	Status	Planned Actions
FY08-OIG-IT-01 Security Controls Testing	Open	**By January 15, 2009, the CSB will:** Test approximately one-third of unique security controls and an Agency-defined set of key controls.
FY08-OIG-IT-02 C&A Process	Open	**By September 30, 2008, the CSB will:** Update the current C&A documentation to include revision history information such as date of revision, individual that updated the document, and description of the revision.
FY08-OIG-IT-03 Privacy Impact and Management	Open	**By October 17, 2008, the CSB will:** Insert into individual database application systems within the CSB's GSS a banner indicating the system is a government system and therefore, similar to the banner presented at logon to the GSS itself.
FY08-OIG-IT-04 Configuration Management	Open	**By October 10, 2008, the CSB will:** Update the security policy and associated procedures to address reviewing, approving and documenting non-standard security configurations.