U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2009)

Report No. 10-P-0174

August 2, 2010

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SP	Special Publication

U.S. Environmental Protection Agency
Office of Inspector General

10-P-0174
August 2, 2010

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We performed this review to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act of 2002 (FISMA).

Background

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) contracted with KPMG, LLP, to perform the Fiscal Year (FY) 2009 FISMA assessment. The evaluation adhered to the Office of Management Budget (OMB) reporting guidance for microagencies, which CSB is considered. We also performed additional procedures to assess the information security program at CSB.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2010/20100802-10-P-0174.pdf

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2009)

What KPMG Found

During our FY 2009 evaluation, KPMG noted that CSB does have an information security program in place that appears to be functioning as designed. We also noted that CSB does take information security weaknesses seriously, as three of the four prior year issues were closed. However, during this year's assessment, we identified areas where CSB could improve upon its Risk Assessment, System Security Planning, Plans of Action and Milestones, Contingency Planning, Access Controls, and Audit Logging practices.

In addition to reviewing CSB's information security practices, KPMG conducted a network vulnerability test of key CSB system and network devices. This test revealed vulnerabilities related to insecure system protocols, default configurations, and unpatched devices. While Board Order 034 provides policies and procedures for maintaining device security, CSB personnel did not always follow this guidance to ensure that network devices were appropriately secured as prescribed. Insecure protocols, default configurations, and unpatched devices significantly elevate CSB's risk of system and data compromise by unauthorized users, which could lead to the alteration or deletion of critical data and a degradation of system performance. KPMG provided the network vulnerability results to CSB management and CSB worked diligently to remediate the identified weaknesses.

What KPMG Recommends

KPMG recommends that CSB:

- Provide appropriate training to CSB individuals responsible for completing the Information Technology System risk assessment, security plan, and access control procedures.
- Develop, maintain, and periodically test the Information Technology System contingency plan in accordance with Board Order 034 and federal guidance.
- Develop a process to maintain access approval requests for the Information Technology System.
- Update Board Order 034 to document a process for maintaining information security Plans of Action and Milestones.

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

THE INSPECTOR GENERAL

August 2, 2010

MEMORANDUM

SUBJECT: Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2009)
Report No. 10-P-0174

FROM: Arthur A. Elkins, Jr.
Inspector General

TO: The Honorable Rafael Moure-Eraso, Ph.D.
Chairman and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board

This final report on the above subject area summarizes the results of information technology security work performed by KPMG, LLP, under the direction of the U.S. Environmental Protection Agency's Office of Inspector General (OIG). The report also includes KPMG's completed Fiscal Year 2009 Federal Information Security Management Act Reporting Template, as prescribed by the Office of Management and Budget.

The estimated cost for performing this audit, which includes contract costs and OIG contract management oversight, is $113,478.

If you or your staff have any questions regarding this report, please contact Rudolph Brevard at (202) 566-0893 or brevard.rudy@epa.gov; or Gina Ross, Project Manager, at (202) 566-1041 or ross.gina@epa.gov.

August 2, 2010

SUBJECT: Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act for Fiscal Year 2009

THRU: Arthur A. Elkins, Jr.
Inspector General
U.S. Environmental Protection Agency

TO: The Honorable Rafael Moure-Eraso, Ph.D.
Chairman and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board

Attached is the KPMG, LLP, final report on the above subject audit. KPMG, LLP, performed the Federal Information Security Management Act (FISMA) evaluation on behalf of the U.S. Environmental Protection Agency. This report includes the test results for selected minimally required information security controls defined by the National Institute of Standards and Technology and the Office of Management and Budget FISMA reporting template for microagencies.

If you or your staff have any questions regarding this report, please contact Rudolph Brevard at (202) 566-0893 or brevard.rudy@epa.gov; or Gina Ross at (202) 566-1041 or ross.gina@epa.gov.

Table of Contents

Appendices

Purpose

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) initiated this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year (FY) 2009. The OIG contracted with KPMG, LLP, to conduct the audit.

Background

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA (the Federal Information Security Management Act), focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). It is supported by security policy promulgated through Office of Management and Budget (OMB), and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) Special Publication (SP) series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

Scope and Methodology

The scope of our testing included CSB Information Technology System, the only CSB information technology system that is subject to FISMA reporting requirements.

We conducted our testing through inquiry of CSB personnel, observation of activities, inspection of relevant documentation, and the performance of limited technical security testing. Some examples of our inquiries with agency management and personnel included, but were not limited to, the process for documenting system security plans, processing user access, and the configuration management process. Examples of our observations included, but were not limited to, viewing access control settings on-screen, and viewing access control settings for portable and mobile devices. Some examples of the documents inspected included, but were not limited

to, the CSB Information Technology System security plan and CSB Board Order 034, *Information Technology Security Program*.

We performed a network vulnerability assessment of CSB's network infrastructure. We used a commercially available tool that tests networked information resources for commonly known vulnerabilities. We provided the results of this testing to CSB management separately.

We performed this evaluation in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States.

Findings

During our FY 2009 evaluation, we noted that CSB does have an information security program in place that appears to be functioning as designed. We also noted that CSB does take information security weaknesses seriously, as three of the four prior year issues were closed. However, during this year's assessment, we identified areas where CSB could improve upon its Risk Assessment, System Security Planning, Plans of Action and Milestones (POA&M), Contingency Planning, Access Controls, and Audit Logging practices.

In addition, we conducted a network vulnerability assessment of key CSB system and network devices. Our tests revealed vulnerabilities related to insecure system protocols, default configurations, and unpatched devices. While Board Order 034 provides policies and procedures for maintaining device security, CSB personnel did not always follow this guidance to ensure that network devices were appropriately secured as prescribed. Insecure protocols, default configurations, and unpatched devices significantly elevate CSB's risk of system and data compromise by unauthorized users, which could lead to altering or deleting critical data and degrading system performance. We have provided the details of the network vulnerability assessment to CSB management separately.

Risk Assessment

CSB did not document the risk assessment for the Information Technology System in the format outlined by National Institute of Standards and Technology (NIST) SP 800-30, *Risk Management Guide for Information Technology Systems.* The Information Technology System risk assessment does not address the requirements for threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, and control recommendations as outlined in the NIST guide. We found CSB officials were not trained in developing risk assessments consistent with NIST. As a result, CSB has a heightened risk of not identifying risks and implementing mitigating controls over CSB's Information Technology System; potentially, system threats and risks could go undetected.

Plans of Action and Milestones

CSB does not have a documented procedure for updating and maintaining a security POA&M for the Information Technology System. Board Order 034 serves as CSB's information security policy, but the policy does not provide guidance on updating the security POA&M. We did note

that the existing Information Technology System POA&M is consistent with federal guidance, but a documented procedure for updating the POA&M would further strengthen CSB's information security program. As CSB identifies new vulnerabilities, a documented POA&M procedure would help guide CSB personnel document risk mitigation plans and establish achievable completion dates. Further, should CSB experience turnover in key information security staff, the newer staff may not be as familiar with how to maintain and update the POA&M.

Contingency Plan

CSB does not have a documented and tested contingency plan for the Information Technology System. Board Order 034 documents a policy and procedure for developing and maintaining a system contingency plan. Further, CSB performs some contingency planning activities, including periodically backing up data and rotating backup data to an offsite location. However, CSB has not developed or tested a system-specific contingency plan. CSB management did not commit the resources and leadership required to develop a contingency plan for the Information Technology System. Without a documented and tested contingency plan completed in accordance with NIST guidance, CSB is at increased risk, that should a significant incident occur, CSB would not be able to recover Information Technology System capabilities.

Access Control

CSB does not consistently maintain records for granting access to the Information Technology System. We reviewed documentation supporting access approvals for 13 percent (5 of 40) Information Technology System users. We found a lack of supporting documentation for every user. Lack of training on the access approval and retaining the supporting documentation process led to access approval supporting documentation not being maintained. By not maintaining documentation supporting system accesses, CSB is at increased risk that system users are not granted access in accordance with management's request.

Audit Logs

CSB has not developed a procedure for performing and documenting log reviews for the Information Technology System. According to CSB officials, security staff members perform a weekly review of Information Technology System audit logs. However, CSB has not documented a specific procedure for performing those audits in accordance with NIST guidance or Board Order 034. The lack of documented procedure for performing system audit log reviews increases CSB's risk that information system security personnel will not conduct the log reviews in a consistent manner, which could lead to increased risk of not detecting key security violations and events.

Recommendations

We recommend that the Chairman, U.S. Chemical Safety and Hazard Investigation Board:

1. Provide appropriate training to CSB individuals responsible for completing the Information Technology System risk assessment. The training should encompass required risk assessment elements.

2. Perform and document the Information Technology System risk assessment in full accordance with NIST SP 800-30 as required by FISMA and CSB policy.

3. Enhance Board Order 034 to document a procedure for developing and maintaining the security POA&M for the Information Technology System.

4. Provide training to key CSB officials on maintaining the POA&M consistent with the documented Board Order 034 procedure.

5. Develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.

6. Provide training to CSB management officials on the need to maintain user access documentation in accordance with Board Order 034 and NIST guidance.

7. Ensure that access approval documentation is maintained for the Information Technology System.

8. Document an audit log review procedure in Board Order 034 consistent with NIST 800-92. The procedure should describe, at a minimum, which system audit logs are to be reviewed, the frequency of log reviews, the process for documenting the reviews, and any escalation procedures needed should a security violation or other event be identified.

9. Provide training to security analysts responsible for complying with Board Order 034 device security requirements.

10. Conduct periodic vulnerability scans to assess device security.

Agency Response and KPMG Comments

In general, CSB agreed with our findings and recommendations. However, CSB disagreed with recommendations related to the prior year audit finding to implement a process for effectively tracking key changes to the Information Technology System security plan. CSB believed that it completed all actions related to the Fiscal Year 2008 recommendations. We reviewed CSB's actions to address the recommendations and concluded that sufficient actions had been taken to address these two recommendations. As a result, we removed the two recommendations from the final report.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	4	Provide appropriate training to CSB individuals responsible for completing the Information Technology System risk assessment. The training should encompass required risk assessment elements.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
2	4	Perform and document the Information Technology System risk assessment in full accordance with NIST SP 800-30 as required by FISMA and CSB policy.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
3	4	Enhance Board Order 034 to document a procedure for developing and maintaining the security POA&M for the Information Technology System.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
4	4	Provide training to key CSB officials on maintaining the POA&M consistent with the documented Board Order 034 procedure.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
5	4	Develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
6	4	Provide training to CSB management officials on the need to maintain user access documentation in accordance with Board Order 034 and NIST guidance.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
7	4	Ensure that access approval documentation is maintained for the Information Technology System.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
8	4	Document an audit log review procedure in Board Order 034 consistent with NIST 800-92. The procedure should describe, at a minimum, which system audit logs are to be reviewed, the frequency of log reviews, the process for documenting the reviews, and any escalation procedures needed should a security violation or other event be identified.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
9	4	Provide training to security analysts responsible for complying with Board Order 034 device security requirements.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			
10	4	Conduct periodic vulnerability scans to assess device security.	O	Chairman, U.S. Chemical Safety and Hazard Investigation Board			

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Microagency Reporting Template

Microagency Reporting Template for FY 2009 FISMA and Information Privacy Management		
Agency Name:	**Chemical Safety and Hazard Investigation Board**	
Agency Point of Contact:	Ana Johnson	
Microagencies are defined as agencies employing 100 or fewer Full Time Equivelent 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	37
f.	Number of contractors	3
g	Number of employees and contractors who received IT security awareness training in the last year	40

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)	Yes
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

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)	http://www.csb.gov/index.cfm?folder=contact_information&page=index
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)	http://www.csb.gov/index.cfm?folder=contact_information&page=index.

Appendix B

Agency Response to Draft Report

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

William B. Wark
Board Member

William E. Wright
Board Member

May 27, 2010

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 your draft report on the independent evaluation of the Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Management Act (FISMA).

The CSB believes it completed all actions from the Fiscal Year (FY) 2008 FISMA recommendations; however, the draft report characterizes actions for one of the prior recommendations as not fully addressing the finding. I will address this below as it is a matter of disagreement with the current FISMA findings and recommendations. Overall, we agree with the majority of the findings and recommendations in the draft FY 2009 FISMA report. The attached table details the CSB's planned actions to address each finding and milestones for completion. Moreover, 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.

The CSB disagrees with recommendations 3 and 4 of the draft report, which state:

> 3. Update Board Order 034, *Information Technology Security Program*, to include a requirement and procedure for maintaining system security documents, notably security plans, with key elements such as the description of the last document change.
>
> 4. Update the Information Technology System security plan to record a description of the last document change.

The draft report's findings state that the "CSB did not fully address the prior year audit finding to implement a process for effectively tracking key changes" to the Information Technology System security plan" (ITSSP). The ITSSP serves as Appendix G to the CSB's Board Order 34, which according to section 33 of the order is reviewed annually and any amendments submitted for Board approval "by March 31 of each year." Revised versions and new sections of the order

are presented to the Board for approval using a formal notation item process. The notation items document—in detail—all changes to the Board Order and are readily available to all reviewers.

Pursuant to the recommendations in the CSB's FY 2008 FISMA evaluation, the CSB improved the format of Board Order 34 to note the dates of all approved amendments to the order and to the ITSSP specifically. When cross referenced with the notation items, these dates provide detailed traceability to the approved changes to the ITSSP and other system security documents. While the use of notation items may not be a process the auditors typically see, we believe it readily enables reviewers to see changes to the system security documents.

Please contact Allen Smith at 202-261-7638, or Charlie Bryant at 202-261-7666 for further information on any of these items.

Sincerely,

JBresland

John S. Bresland
Chairman and CEO

Enclosure

CSB Comments and Planned Actions on Draft FY 2009 FISMA Findings

FY 2009 FISMA Finding	Status	Recommendation	CSB Response	Planned Actions
FY09-OIG-IT-01-01 Information Technology System Risk Assessment	Open	Provide appropriate training to CSB individuals responsible for completing the Information Technology System risk assessment. The training should encompass risk assessment elements required by SP 800-30.	Agreed. CSB IT personnel are educated on the risk assessment process, but we will evaluate training options to strengthen our risk assessment program.	Evaluate training options for strengthening the CSB's risk assessment program to include SP 800-30 and develop appropriate training plans.
FY09-OIG-IT-01-02 Information Technology System Risk Assessment	Open	Perform and document the Information Technology System risk assessment in full accordance with NIST SP 800-30 as required by FISMA and CSB policy.	Agreed. CSB has historically been using a risk assessment form developed by IMTS, an information security consultant; however, the CSB will modify/update its internal risk assessment to conform to NIST SP 800-30.	1) Update the current CSB risk assessment reporting form to reflect NIST SP 800-30 guidance; and 2) Conduct a risk assessment with the updated materials.

Summary of FY 2009 Draft Findings & CSB Planned Actions

FY 2009 FISMA Finding	Status	Recommendation	CSB Response	Planned Actions
FY09-OIG-IT-02-01 Information Technology System Security Plan Maintenance	Disagree	Update Board Order 034, *Information Technology Security Program*, to include a requirement and procedure for maintaining system security documents, notably security plans, with key elements such as the document version and the description of the last document change.	The CSB does not concur. The main concern raised in the finding is the ability of CSB officials to discern whether they are "working with the correct version of the security plan." According to section 33 of Board Order 34, the Board Order is reviewed annually and any amendments submitted for Board approval "by March 31 of each year." A new version is memorialized upon Board approval of the amended order. Notation Items—the formalized process by which Board Orders are amended--are available on the CSB website. Click here to view the last approved change to Board Order 34. The approval date is subsequently added to the last page of the Board Order, and also to any amended appendix—if that is the only section amended. In any event, the current system allows CSB officials to know which version is current. Also, prior versions can be accessed for reference if needed.	None.
FY09-OIG-IT-02-02 Information Technology System Security Plan Maintenance	Disagree	Update the Information Technology System security plan to reflect the document version and description of the last document change.	The CSB does not concur. See comments for FY09-OIG-IT-02-01.	None

Summary of FY 2009 Draft Findings & CSB Planned Actions

FY 2009 FISMA Finding	Status	Recommendation	CSB Response	Planned Actions
FY09-OIG-IT-03-01 Information Technology System Plan of Action and Milestones (POA&M)	Open	Enhance Board Order 034 to document a procedure for developing and maintaining the security POA&M for the Information Technology System.	Agreed.	Update Board Order 34 to include a procedure for developing and maintaining the security POA&M for the Information Technology System.
FY09-OIG-IT-03-02 Information Technology System Plan of Action and Milestones (POA&M)	Open	Provide training to key CSB officials on maintaining the POA&M consistent with the documented Board Order 034 procedure.	Agreed.	Complete training on Board Order 34 POA&M procedure.
FY09-OIG-IT-04 Information Technology System Contingency Plan	Open	We recommend CSB management develop, maintain, and periodically test a contingency plan for the Information Technology System in accordance with CSB Board Order 034 and NIST guidance.	Agreed. The CSB has already convened a workgroup tasked with developing this plan.	Develop a draft Contingency Plan consistent with Board Order 34 and NIST SP 800-34.
FY09-OIG-IT-05-01 Information Technology System Access Approvals	Open	Provide training CSB management officials on the need to maintain user access documentation in accordance with Board Order 034 and NIST guidance.	Agreed. The CSB will conduct training on the access control policy and procedure in Board Order 34.	Conduct training on access control pursuant to the guidance in Board Order 34.

Summary of FY 2009 Draft Findings & CSB Planned Actions

FY 2009 FISMA Finding	Status	Recommendation	CSB Response	Planned Actions
FY09-OIG-IT-05-02 Information Technology System Access Approvals	Open	Ensure that access approval documentation is maintained for the Information Technology System.	Agreed.	Update Board Order 34 to include a procedure to maintain an easily accessible user access log.
FY09-OIG-IT-06 Audit Log Review Procedure	Open	We recommend that CSB document an audit log review procedure in Board Order 034 consistent with NIST 800-92. The procedure should describe, at a minimum, which system audit logs are to be reviewed, the frequency of log reviews, the process for documenting the reviews, and any escalation procedures needed should a security violation or other event be identified.	Agreed. The CSB has already convened a workgroup tasked with developing this procedure.	Update Board Order 34 to include an audit log review procedure consistent with NIST 800-92.
FY09-OIG-IT-07-01 Internal Security Vulnerabilities	Open	1) Provide training to security analysts responsible for complying with Board Order 034 device security requirements.	Agreed. CSB will train on amended procedure prescribed in FY09-OIG-IT-07-02.	Conduct training on vulnerability scans pursuant to the guidance in Board Order 34.
FY09-OIG-IT-07-02 Internal Security Vulnerabilities	Open	2) Conduct periodic vulnerability scans to assess device security.	Agreed. The CSB conducts periodic scans; however, these scans were not comprehensive enough regarding certain network devices. CSB will amend its procedure to ensure more comprehensive vulnerability scans of all network devices. Please note that the threats identified during the vulnerability scans were immediately corrected.	Amend procedure for periodic vulnerability scans to ensure more comprehensive scans of network devices.