

**U.S. CHEMICAL SAFETY AND HAZARD
INVESTIGATION BOARD**

Office of Inspector General

INFORMATION TECHNOLOGY:

Information Security Program
Evaluation, FY2003



Office of Information Technology

OIG-IT-03-03

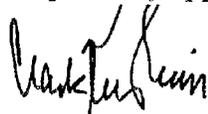
September 2003

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein, if any, have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.



Clark Kent Ervin
Acting Inspector General

Contents

Introduction	3
Results in Brief	4
Results of Independent Evaluation... ..	5
Overview of FISMA IT Security Reviews.....	5
Responsibilities of Agency Head.....	9
Responsibilities of Agency Program Officials and Agency Chief Information Officer.....	14
Appendices	
Appendix A: Purpose, Scope, and Methodology.....	18
Appendix B: Documents Reviewed by OIG and KPMG	19

Introduction

The Office of Inspector General (OIG) tasked KPMG LLP (KPMG) to assist in performing the FY 2003 Federal Information Security Management Act (FISMA) independent evaluation of the United States Chemical Safety and Hazard Investigation Board's (CSB) information security program and practices. CSB is a small federal entity and as a result, does not have an information security program and related practices comparable to those of larger federal entities, and this has been taken into account during the evaluation.

To perform the independent evaluation, we requested all documentation related to prior CSB audits, security evaluations, security program reviews, vulnerability assessments, and other reports addressing CSB's information security program and practices. In addition, documentation supporting security training, security-related capital planning efforts for technology, memoranda regarding information security policies, and plans for future information security assessments was requested. Appendix B lists the documents that were obtained and reviewed as part of this evaluation. From the information received, we evaluated CSB's progress in meeting Office of Management and Budget (OMB) performance measures.

financial resources has prevented this issue from being addressed (Security Implementation material weakness).

OIG reviewed the results with CSB management who concurred with our independent evaluation and findings..

Results of Independent Evaluation

A. Overview of FISMA IT Security Reviews

A.1-Identify the agency's total IT security spending and each individual major operation division or bureau's IT security spending as found in the agency's FY03 budget enacted.

OIG is not required to report on this area.

performed one IT security self-assessment. The methods used to assess the programs included the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 Self Assessment Guide and the Cost Estimation, Benchmarking, and Risk Assessment (COBRA) tool. CSB completed and documented all questions in the self-assessment; it reflects the current CSB information security conditions.

During FY 2003, CSB continued to use the Bureau of Public Debt (BPD) to process its finances, and the National Business Center (NBC) to process employee payroll. Periodically, CSB's IT Security Officer reviews the connection between CSB, BPD and NBC to ensure it is secure and meets CSB's encryption standards.

A.3- Material Weaknesses

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.				
Bureau Name	FY03 Material Weaknesses			
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
CSB	3	2	Security Policy Security Implementation	Yes
Agency Total	3	2		

Based on our review, CSB has two material weaknesses. These were noted in the FY 2002 GISRA report and continue to exist. CSB's GISRA FY 2002 report submission included four material weaknesses:

1. Security policy
2. Security implementation
3. Security monitoring
4. Continuous security improvement

These four material weaknesses are documented in CSB's Plan of Action and Milestones (POA&M). CSB has taken numerous steps to address the weaknesses noted above. The security policy material weakness primarily relates to the *CSB Information Technology Security Plan*, which is currently in draft and is expected to be completed by the end of October 2003. Until this plan is completed, communicated to all employees, and operating effectively, CSB will continue to have a material weakness related to its security policy.

CSB has an ITSO who is responsible for the development, implementation, and management of the agency-wide security POA&M process. Agency program officials, in coordination with the CSB Chief Operating Officer (COO)¹, develop, implement, and manage POA&Ms for the CSB systems they own and operate (i.e., systems that support their programs). The agency program officials and the agency COO report to OMB the status of the POA&Ms on a quarterly basis. The POA&M is the authoritative agency management tool to identify and monitor agency actions. The current CSB POA&M (dated August 12, 2003) is up-to-date and is used for tracking corrective actions. In addition, the POA&M includes the funding requirements for the specific system level POA&M activities. Finally, the POA&M contains a scheduled completion date, as well as a status column. The status indicates that the milestones were either completed, on hold, or on-going. The four milestones that are on hold are in this status since funding for completing the milestone has not been approved.

B. Responsibilities of Agency Head

B.1 - Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?

The COO has assigned FISMA responsibilities to the ITSO. The ITSO was also responsible for the completion of the FY 2001 and FY 2002 GISRA reports. CSB is a small agency and the agency's COO manages the agency's IT program. The task of consolidating the agency's FISMA security self-assessment and POA&M efforts has been delegated to the ITSO. Having the ITSO responsible for FISMA related tasks is an effective control over the CSB security program. From an information security perspective, the CSB organizational structure is sufficient.

B.2 – Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

CSB recently completed its agency-wide IT capital planning process implementation. This process was initiated based on the FY 2002 GISRA review.

¹ Because of its size, CSB does not have a Chief Information Officer (CIO) position. The COO serves in this role.

other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?

CSB is a small agency and has one security program. The security program is centrally managed through the IT office, thus precluding any duplication of overhead costs of different personnel working on information security tasks.

B.7 –Critical Operations and Assets

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	Yes		No	X
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes		No	X
c. Has the agency fully identified its mission critical operations and assets?	Yes	X	No	
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes	X	No	
e. If yes, describe the steps the agency has taken as a result of the review.	An informal approach was used to classify CSB IT assets as high criticality, high availability, and high integrity. However, the approach was not documented.			
f. If no, please explain why.	CSB states it has no national critical systems. We note that no organizational security risk assessment has been performed on CSB's IT assets or systems.			

The lack of a documented assessment of CSB's critical operations and assets is another part of the security implementation material weakness.

CSB's draft security program plan documents incident detection and response procedures. The procedures note that the CSB ITSO will develop procedures for incident handling and responses. While these procedures are being developed, CSB has informally adopted the FedCIRC procedures. CSB should document these procedures. Until that time, the COO should issue a memorandum formally adopting FedCIRC incident reporting procedures.

B.9 – Number of Security Incidents

B.9 Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.			
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
CSB	111,000	2	1

CSB estimates the number of incidents, including very minor ones, coming via the internet, to be 111,000 during FY 2003. During the internal and external vulnerability assessment performed on CSB's information systems, this number was determined to be reasonable due to the extremely high level of sensitivity at which CSB's host-based and network-based intrusion detection systems are configured. CSB's network intrusion detection system will note even small events, such as a ping.

Of the many "incidents" identified, only two were reported to FedCIRC during FY 2003, and just one of those to law enforcement. The incident reports provided sufficient evidence that CSB is reporting to FedCIRC and when necessary, reporting to law enforcement.

official must authorize systems to process. Such a process also helps ensure that security controls are implemented throughout a system life cycle in accordance with organizational security policy and Federal guidelines and requirements, and that management accepts the risk of the system operating.

The CSB IT contingency plan covers all three systems, identifies ten technologies² used at CSB and the related failsafe methodologies supporting these technologies. Periodic tests of the CSB failsafe technologies have taken place to ensure that various backup processes would be effective. The contingency plan does not refer to a hot site or alternate processing facilities, but this is appropriate given CSB's small IT environment and reliance on service providers for key processes (i.e., payroll and financial processing).

C.2- Agency-Wide Security Program

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.				
Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
No	Yes	No	Yes	Yes

The CSB security plan is in draft and has not been finalized or approved by CSB management. The creation and development of the security plan is one of the main tasks assigned to the ITSO. CSB is planning to complete the security plan by October 2003. Until that time, CSB will not be able to ensure that CSB complies with the agency-wide IT security program.

CSB currently maintains one POA&M. As noted previously, each of the three program areas uses the same IT systems to complete their respective tasks. The POA&M, updated on August 12, 2003 for the FY 2003 FISMA review, consists of 14 action items. Each item has a designated point of contact, resources required (if applicable), recommendations, milestones, and the date when the issue was identified. The CSB POA&M addresses the FY 2002 GISRA findings and recommendations. In addition, it is a comprehensive document addressing all weaknesses noted in prior year CSB security reviews. Further, the POA&M contains a scheduled completion date, as well as the status. The status indicates

² CSB technologies include uninterruptible power supply, RAID implementation, secondary electronic mail server, and differential and full backups of CSB servers.

C.4 - Capital Planning and Investment

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
CSB	3 planned to be reported	Yes	Yes	Yes

It was noted during the FY 2002 GISRA evaluation that according to the CSB Charter, CSB is not required to submit capital planning documents to OMB. For FY 2003, CSB has an Agency IT Investment Portfolio, which they will use to submit system funding requests to OMB. The CSB IT capital plan documents the Agency IT Investment Portfolio, and includes the security needs to support the agency IT portfolio. CSB's small size allows for CSB management to be directly involved in the approval of IT expenditures, including security related expenditures.

We would like to extend our appreciation to CSB for the cooperation and courtesies extended to our staff during the review. If you have any questions, please feel free to contact me at (202) 254-4044, or Frank Deffer, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4100.

1. FedCIRC Reporting Requirements
2. CSB NIST Self Assessment
3. CSB Agency Structure Chart
4. POA&M, dated August 12, 2003
5. Draft Version of *Information Technology Security Program Plan*
6. *Information Technology Contingency Plan*
7. Computer Security Policies, Procedures, and Rules of Behavior
8. CSB's Draft Responses to FISMA Questionnaire
9. FY 2002 OIG GISRA Executive Summary
10. Sample certifications for CSB IT Manager/Security Officer
11. Sample messages related to security awareness and virus attack communication
12. CSB incident reports sent to FedCIRC
13. Draft IT capital planning document
14. E-mails sent to the CSB IT Manager/Security Officer informing CSB of security threats
15. FedCIRC Patch Authentication and Dissemination Capability Form

