



Office of Inspector General

~~SENSITIVE BUT UNCLASSIFIED~~

**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Office of Audits

**Evaluation of the United States Section,
International Boundary and Water Commission,
Information Security Program**

Report Number AUD/IT-12-16, November 2011

~~Important Notice~~

~~This report is intended solely for the official use of the Department of State of the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. § 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~SENSITIVE BUT UNCLASSIFIED~~



United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report is being transmitted pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed a review of the United States Section, International Boundary and Water Commission Information Security Program for FY 2011. The report is based on interviews with employees and officials of the United States Section, International Boundary and Water Commission headquarters and field offices, direct observation, and a review of applicable documents.

OIG identified areas in which improvements could be made, including the system inventory, risk management program, configuration management, security awareness and role-based training, plans of actions and milestones, remote access, continuous monitoring, contingency planning, oversight of contractor systems, security capital planning, [REDACTED]

The recommendations contained in the report were developed on the basis of the best knowledge available and were discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of the individuals who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel", written in a cursive style.

Harold W. Geisel
Deputy Inspector General

Acronyms

| | |
|-------|--|
| CM | configuration management |
| COOP | Continuity of Operations |
| FISMA | Federal Information Security Management Act |
| GSS | General Support System |
| IBWC | United States Section, International Boundary and Water Commission |
| IMD | Information Management Division |
| IT | information technology |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| POA&M | Plan of Action and Milestones |
| SP | Special Publication |
| SSP | system security plan |

Table of Contents

| | |
|---|----|
| Executive Summary | 1 |
| Background..... | 4 |
| Results of Evaluation | 6 |
| A. System Inventory | 6 |
| B. Risk Management Program..... | 7 |
| C. Configuration Management..... | 9 |
| D. Security Training..... | 10 |
| E. Plan of Action and Milestones | 12 |
| F. Remote Access..... | 13 |
| G. Continuous Monitoring..... | 14 |
| H. Contingency Planning..... | 17 |
| I. Oversight of Contractor System | 19 |
| J. Security Capital Planning..... | 20 |
| | 21 |
| | 22 |
| List of Recommendations | 25 |
| Appendices | |
| A. Objectives, Scope, and Methodology | 28 |
| B. Followup of Recommendations From the FY2010 Federal Information Security Management Act Report..... | 29 |
| | 30 |
| | 34 |
| E. International Boundary and Water Commission Response..... | 39 |
| Major Contributors to This Report | 49 |

Executive Summary

In accordance with the Federal Information Security Management Act (FISMA) of 2002,¹ the Department of State, Office of Inspector General (OIG), performed an independent evaluation of the United States Section, International Boundary and Water Commission (IBWC), information security program and practices to determine compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Additionally, the results are designed to assist OIG in providing responses to OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

OIG reviewed remedial actions taken by IBWC to address the FY 2010 reported FISMA control weaknesses identified in the independent public accounting firm's FY 2010 report *Audit of the International Boundary and Water Commission Federal Information Security Management Act*. The statuses of the recommendations from the FY 2010 report are presented in Appendix B.

Overall, OIG found that IBWC had implemented an information security program but identified weaknesses that, if exploited, could significantly impact the information security program controls and expose IBWC to security breaches. The weakened security controls could adversely affect the confidentiality, integrity, and availability of IBWC information and information systems. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, IBWC needs to address the control weaknesses identified.

A. System Inventory

IBWC has not implemented a process or procedure to update and manage its information technology (IT) assets. Although IBWC performed an inventory of its hardware and systems during FY 2011, it did not fully account for all assets. Without a process to properly identify, document, and maintain an inventory of systems, IBWC may not have an accurate accounting of all IT assets and related system interfaces and underlying support systems.

B. Risk Management Program

IBWC's risk management program for information security needs improvement at the organization and system levels. At the organizational level, IBWC had not implemented a risk management framework and information security policies and procedures that describe the roles and responsibilities of key participants. In addition, there is no governance structure in place to address risk within IBWC. Further, IBWC had not

¹ Pub. L. No. 107-347, title III.

developed an IT strategic plan or enterprise architecture that shows the IT goals for the organization or links the strategic goals and objectives to the defined business functions.

At the system level, IBWC had not completed security assessment and authorization (formerly certification and accreditation) of its Supervisory Control and Data Acquisition (SCADA) systems. IBWC was not aware of the requirements to complete the security assessment and authorization process for the SCADA systems. OIG found that only one of two systems was certified and accredited by year end. Additionally, the security authorization package for the general support system (GSS) was not reassessed after a significant change. These conditions weaken IBWC's risk management framework to assess, respond to, and monitor information security risk.

C. Configuration Management

IBWC had not implemented an effective patch management process to evaluate patches for applicability, process of installation, monitoring, and periodic review of the patch statuses on the systems. Without detailed procedures that govern the performance of the configuration management processes, IBWC may not be able to manage effectively the IT security program, which may lead to the introduction of security weaknesses and inconsistent performance.

D. Security Training

Although the IBWC security awareness training program requires all personnel to complete annual security awareness training and users with significant security responsibilities to complete specialized training, OIG found that IBWC employees had not completed their general security awareness training and employees who have significant security responsibilities had not completed their specialized training.

E. Plan of Action and Milestones

IBWC had not effectively implemented a Plan of Action and Milestones (POA&M) process. OIG found that IBWC's POA&M policy and procedures had not been formally adopted by management. In addition, IBWC's POA&Ms did not identify the estimated resource requirements and corrective action plans to close the POA&M deficiencies.

F. Remote Access

IBWC had not developed and implemented a remote access policy and procedure to comply with NIST requirements. Without proper policies and procedures, individuals may introduce vulnerabilities into the IBWC network.

G. Continuous Monitoring

IBWC had not developed a means to implement continuous monitoring of its IT systems. Specifically, IBWC had not performed routine security assessments of its systems or periodic vulnerability scans. Without periodic reviews or the performance of risk-based

security assessments, new threats and vulnerabilities may not be identified and mitigated in a timely manner.

H. Contingency Planning

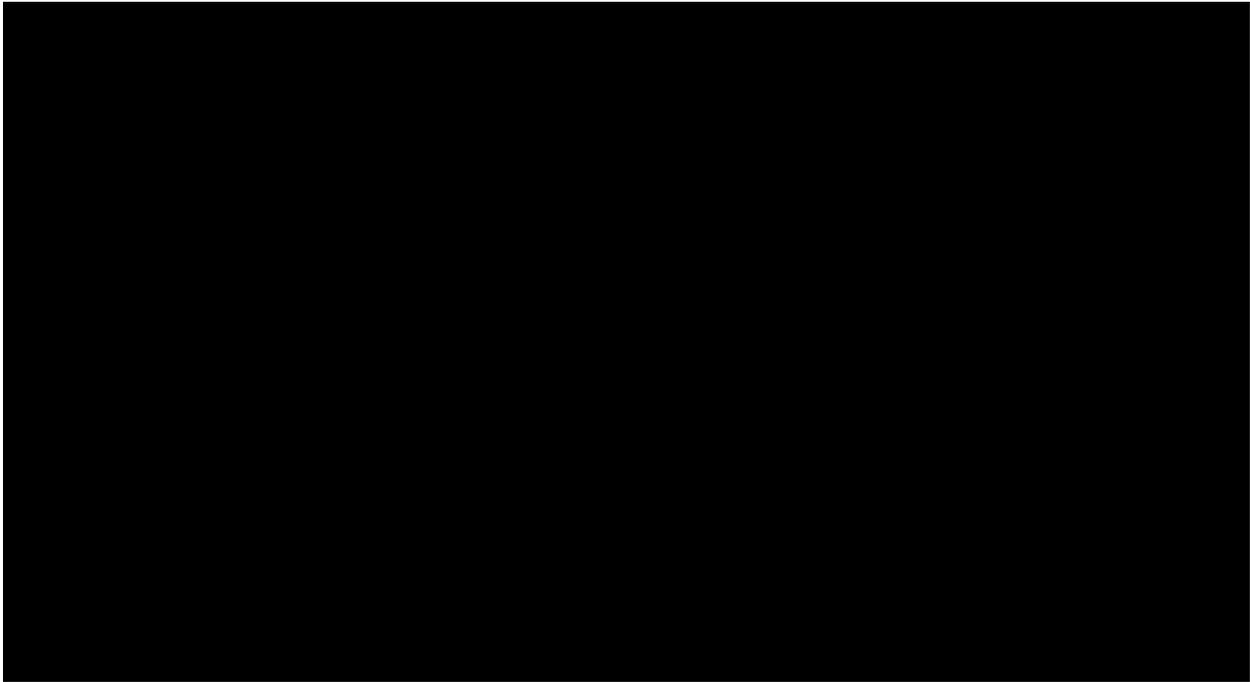
IBWC's Continuity of Operations (COOP) does not comply with NIST Special Publication (SP) 800-34.² OIG found that the COOP for IBWC's GSS had not been updated or tested after a significant change. Lack of an updated contingency plan may prevent IBWC from accessing critical information and resources and resuming business functions in case of an extended outage and/or disaster.

I. Oversight of Contractor System

IBWC had not implemented an effective oversight program of its contractor system. OIG found that IBWC officials did not have adequate control over the IT functions at the San Diego (CA) waste treatment plant. In addition, IT assets are purchased and maintained by the contractor in support of the operations in San Diego without IBWC Information Management Division (IMD) review and approval.

J. Security Capital Planning

Information security is not integrated into IBWC's Capital Planning and Investment Control process. IBWC did not provide OMB with a detailed explanation for the major investment related to its IT assets. Inadequate planning increases the risk that requests for funding investments will not receive proper consideration.



OIG made 21 recommendations, including the three recommendations included in OIG's August 26, 2011, Outline for Action that pertained to personnel security and physical and environmental protection (Findings K and L, respectively). The other significant security deficiencies requiring immediate attention are in the risk management program (Finding B), security configuration management (Finding C), plans of action and milestones (Finding E), continuous monitoring (Finding G), and oversight of the contractor system (Finding I).

IBWC concurred with all the recommendations. Based on the information provided, OIG considers all 21 recommendations resolved, pending further action. IBWC's responses and OIG's replies are presented after each recommendation.

Background

IBWC is an international organization created in 1889 by the Governments of the United States and Mexico to administer the boundary and water rights treaties and agreements between the two countries.

The entity was created as the International Boundary Commission by the Convention of 1889³ and given its current name under the Treaty of 1944.⁴ IBWC consists of the United States Section and the Mexican Section, which have their headquarters in the adjoining cities of El Paso and Ciudad Juárez, Chihuahua, respectively. Although IBWC is an independent international entity, the United States Section takes direction from the Department of State on matters related to foreign policy. The Mexican Section is a unit in the Mexican Ministry of Foreign Affairs.

IBWC is charged through a series of treaties and agreements with the application, regulation, and exercise of the provisions of such treaties and agreements for the solution of water and boundary issues along the 1,954-mile border between the two countries. The United States Section of IBWC operates under the provisions of 22 U.S.C. 277.⁵ The mission of the United States Section working jointly with the Mexican Section is as follows:

- Distribute the waters of the boundary rivers between the two countries.
- Operate international flood control along the boundary rivers.
- Operate the international reservoirs for conservation and regulation of Rio Grande waters for the two countries.

³ The Convention of 1889 was to avoid the difficulties occasioned by reason of the changes that take place in the beds of the Rio Grande and Colorado River, U.S.-Mex., March 1, 1889, 26 Stat. 1512 (extended indefinitely by Article two of treaty signed Feb. 3, 1944.) (59 Stat. 1219)).

⁴ Treaty of 1944 relates to utilization of waters of the Colorado and Tijuana Rivers and of the Rio Grande, and supplementary protocol, U.S.-Mexico, Feb. 3, 1944. (59 Stat. 1219).

⁵ 22 U.S.C. § 277, "International Boundary Commission, United States and Mexico; study of boundary waters."

- Improve the quality of water of international rivers.
- Resolve border sanitation issues.
- Develop hydroelectric power.
- Establish the boundary in the area I imitrophe to (bordering) the Rio Grande.
- Demarcate the land boundary.

The Federal Information Security Management Act of 2002 (FISMA) was enacted into law as Title III, Public Law Number 107-347 on December 17, 2002. Key requirements of FISMA are as follows:

- The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- An annual independent evaluation of the agency's information security programs and practices.
- An assessment of compliance with FISMA requirements.

FISMA recognized the importance of information security to the economic and national security interests of the United States. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including information and information systems provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

FISMA assigns specific responsibilities to Federal agencies, NIST, OMB, and the Department of Homeland Security (DHS) to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

On an annual basis, OMB provides guidance with reporting categories and questions for meeting the current year's reporting requirements.⁶ OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

⁶ OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated Sept. 14, 2011.

Results of Evaluation

Overall, OIG found that IBWC had implemented an information security program; however, OIG identified weaknesses that, if exploited, could significantly impact the information security program controls and expose IBWC to security breaches. The weakened security controls could also adversely affect the confidentiality, integrity, and availability of information and information systems. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, IBWC needs to address the control weaknesses described.

A. System Inventory

IBWC had not implemented an inventory management process and procedures to update and manage its IT assets. Although IBWC performed an inventory of its hardware and systems during FY 2011, it did not fully account for all assets. OIG found that the IBWC inventory listed only components associated with the GSS and did not include all IT assets. Specifically, OIG identified components in the server room and in the wiring rooms of the first and third floors at the headquarters in El Paso, and at the San Diego field office, that were not recorded in the inventory. In addition, the listing did not include the SCADA systems operated at the IBWC field offices in San Diego and at Falcon and Amistad (TX).⁷

FISMA requires the heads of each agency to develop and maintain an inventory of major information systems operated by or under the agency's control and to identify information systems in an inventory, to include identifying the interfaces between each system and other systems or networks and including those information systems not operated by or under the control of the agency. FISMA further requires the inventory to be updated at least annually and to be used to support information resources management.

Without a system inventory management process for all IT assets, including the SCADA systems, IBWC will not have an accurate accounting of all related system interfaces or underlying support systems and will not be able to properly identify and mitigate security risks. As a result, critical management processes such as strategic planning, budgeting, system administration, and resource management may be adversely affected.

Recommendation 1. OIG recommends that the Chief Information Officer ensure that all assets are accounted for in the inventory system and develop a process that updates, not less than annually, the International Boundary and Water Commission's (IBWC) system inventory when changes are made to those information systems operated by or under the control of IBWC or by third-party contractors or agencies on behalf of IBWC, as required by the Federal Information Security Management Act.

⁷ The SCADA system in San Diego is contractor owned and operated. The SCADA systems in Falcon and Amistad are owned and operated by IBWC. OIG performed fieldwork at the office in San Diego.

Management Response: IBWC concurred with the recommendation, stating that IMD “has initiated the development of its own IT asset inventory, in addition to the one maintained “ in the Department’s ILMS, “in order to accurately account for all IT assets that make up the [GSS] and existing SCADA systems identified” in San Diego, Nogales (AZ), Amistad, and Falcon.

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented a process to accurately account for all IT assets in the inventory system.

B. Risk Management Program

IBWC’s risk management program for information security needs improvement at the organization and system levels. At the organizational and system level, IBWC had not implemented a risk management framework and information security policies and procedures that describe the roles and responsibilities of key participants. As such, OIG could not review the risk management framework and determine how IBWC manages information security risk.

In addition, IBWC did not have a governance structure in place to address risk within the organization and had not developed an IT strategic plan or enterprise architecture that shows the IT goals for the organization or links the strategic goals and objectives to the defined business functions. Further, because the risk management strategy had not been implemented at the organizational level, communication of operations at the system level are negatively affected, along with business decisions such as funding allocation, because management was not fully aware of the security vulnerabilities that exist.

At the information system level, OIG found deficiencies in the security assessment and authorization (formerly certification and accreditation) documentation as follows:

- For the SCADA systems, IBWC had not completed the security assessment and authorization package, as required by NIST SP 800-82⁸ and NIST SP 800-53, Revision 3.⁹
- For the GSS SSP, only one of two systems had been assessed and authorized by year end. The CIO certified the GSS SSP in April 2007. However, several changes have been made to the GSS since that time, including a change to the designated approving authority, the addition of a COOP site, and a change to the transportation mode for information.
- For the GSS SSP, which documents security controls for the system, the security baseline controls were not documented in compliance with NIST SP 800-53, Revision 3, and the security assessment report supporting the independent assessor’s evaluation of management, operational, and technical controls was outdated. IBWC also did not review and document test results of annual subset assessments.

⁸ NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, June 2011.

⁹ NIST SP 800-53, rev. 3, *Recommended Security Controls for Information Systems and Organizations*, Aug. 2009 (last updated May 2010).

- For the authority to operate, which proves that an authorizing official has accepted the identified risk, OIG found that the GSS did not have a full security assessment and authorization performed after significant changes had been made to the network environment. In addition, the GSS authority to operate was not valid because of a change in the designated approving authority.

IBWC did not properly follow guidelines contained in NIST SP 800-37, Revision 1,¹⁰ for properly managing the documentation in the security assessment and authorization packages. An IBWC official stated that IBWC was unaware of the requirement to complete the security assessments and authorization packages for the SCADA systems and the requirement to update the GSS SSP after significant changes were made. These conditions weaken IBWC's risk management framework to assess, respond to, and monitor information security risk.

Recommendation 2: OIG recommends that the Chief Information Officer improve the risk management strategy at the organizational level for assessing, responding to, and monitoring information security risk, as required in National Institute of Standards and Technology Special Publication 800-37, Revision 1.

Management Response: IBWC concurred with the recommendation, stating that the CIO "has initiated steps necessary to bring about an effective risk management framework and policies and procedures in accordance with NIST SP 800-37 Revision 1." IBWC also stated that the IMD "has begun updating the existing System Security Plan to include all current security baseline controls, changes in the GSS and identified SCADA systems." In addition, according to IBWC, the IMD "will prepare a new security assessment and authorization package to apply for and achieve an Authority to Operate designation from the new Designated Authority in FY12."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented a risk management strategy at the organizational level for assessing, responding to, and monitoring information security risk.

Recommendation 3. OIG recommends that the Chief Information Officer:

- Develop the security assessment and authorization packages for the Supervisory Control and Data Acquisition systems, as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-82 and NIST SP 800-53, Revision 3.
- Improve existing procedures to ensure security assessment and authorization packages are updated every 3 years or when a significant change occurs, as required by NIST SP 800-37, Revision 1.

¹⁰ NIST SP 800-37, rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Feb. 2010.

- Improve existing procedures to ensure system security plans and security assessment reports are updated as required to comply with the security baseline controls in NIST SP 800-53, Revision 3.
- Perform annual security assessments of a subset of a system’s security controls, as required by NIST SP 800-37, Revision 1.

Management Response: IBWC concurred with the recommendation, stating that the CIO “will take all necessary action to comply with all items under this recommendation and to comply with NIST SP 800-53, Revision 3, NIST SP 800-37, Revision 1, and SP 800-82.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented all items under this recommendation and has taken actions to comply with the special publications specified.

C. Configuration Management

IBWC had not implemented effective configuration management (CM) standards and procedures for its IT environment. Although IBWC had CM standards and procedures in place, it did not account for the patch management process to evaluate patches for applicability, installation process, monitoring, and periodic review of the patch status on the systems. [REDACTED]

According to NIST SP 800-53, Revision 3, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

NIST SP 800-53, Revision 3, states:

The organization develops, disseminates, and reviews/updates [at an organizational-defined frequency]:

- a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.”¹¹

¹¹ CM-1, “Configuration Management Policy and Procedures.”

An IBWC official stated that the CM standards and procedures are currently being “revamped” but that the draft CM policy and procedures are currently being utilized. Without detailed procedures that govern the performance of the CM processes, IBWC will not be able to effectively manage the IT security program, which could lead to the introduction of security weaknesses and inconsistent performance.

Recommendation 4. OIG recommends the Chief Information Officer develop and implement security configuration management procedures and periodically assess compliance with the implemented procedures, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Response: IBWC concurred with the recommendation, stating that the “draft Configuration Management policy and procedure is currently being reviewed by management for approval by the Commissioner.” IBWC further stated, “ With the acquisition of new security appliances purchased in FY11, the IMD will be able to evaluate patches for applicability, install, monitor and review patch status on all systems in a much more efficient and effective way.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented security configuration management procedures and periodically assessed compliance with the implemented procedures.

Recommendation 5. OIG recommends that the Chief Information Officer develop procedures for the oversight of all systems and hardware that are part of the International Boundary and Water Commission operations, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Response: IBWC concurred with the recommendation, stating that the IMD “has acquired hardware and software that will provide the necessary tools to establish an effective continuous monitoring program.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented procedures for the oversight of all systems and hardware that are part of IBWC operations.

D. Security Training

Although IBWC’s security awareness training program requires all personnel to complete annual security awareness training and users with significant security responsibilities to complete specialized training, OIG found that IBWC employees had not completed their general security awareness training and employees with significant security responsibilities had not completed their specialized training.

OMB Circular No. A-130¹² mandates that agencies provide periodic computer security awareness training to all users as well as specialized training for individuals who have significant security responsibilities. Training ensures that all users are knowledgeable about the rules of the system. However, IBWC officials did not enforce compliance with the security awareness training policy. An IBWC official stated that compliance with training had not been strictly enforced but that IBWC intends to train all employees by the end of the fiscal year.

NIST SP 800-50¹³ states, “at a minimum, the entire workforce should be exposed to awareness material annually. A continuous awareness program, using various methods of delivery throughout the year, can be very effective. Security training for groups of users with significant security responsibility (e.g., system and network administrators, managers, security officers) should be incorporated into ongoing functional training as needed. the organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and thereafter (i.e. at least annually). NIST SP 800-53, Revision 3,¹⁴ states, “[T]he organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.”

Without the completion of initial and annual security awareness training, personnel may be unaware of new risks that may compromise the confidentiality, integrity, and availability of data. As a result, personnel may be unable to recognize and respond appropriately to potential and actual security concerns.

Recommendation 6. OIG recommends that the Chief Information Officer enforce the security awareness training policy requiring all personnel to attend initial and refresher security awareness training and enforce consequences of noncompliance for personnel who do not successfully complete the security awareness training, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and Office of Management and Budget Circular No. A-130.

Management Response: IBWC concurred with the recommendation, stating that the IMD had “conducted five IT Security training classes immediately after the OIG visit in August resulting in 235 employees out of 272 completing their annual IT Security training.” IBWC also stated that the IMD “has also acquired a cloud based training system that will allow for a much more efficient method to provide IT Security training to IBWC personnel.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented security awareness training policy requiring all personnel to attend initial

¹² OMB Circular No. A-130, revised, *Management of Federal Information Resources*, app. III, “Security of Federal Automated Information Resources.”

¹³ NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, pg.20, F/N13, Oct. 2003.

¹⁴ NIST SP 800-53, rev. 3, PS-8 Personnel Sanctions, Aug. 2009.

and refresher security awareness training and enforce consequences of noncompliance for personnel who do not successfully complete the training.

Recommendation 7. OIG recommends that the Chief Information Officer enforce the security awareness training requirement for those personnel with significant security responsibilities, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and Office of Management and Budget Circular No. A-130.

Management Response: IBWC concurred with the recommendation, stating, “Of the eight employees within the agency with significant security responsibilities, five attended training resulting in approximately 63% of employees with significant security responsibilities meeting this requirement. The remaining employees are scheduled to obtain the required in FY12.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented the security awareness training requirement for those personnel with significant security responsibilities.

E. Plan of Action and Milestones

IBWC had not effectively implemented a POA&M process. The implementation of a POA&M process is important to assess the state of the GSS security posture and to aid in oversight of IT investments. Specifically, OIG found the following deficiencies:

- The POA&Ms did not address findings identified during previous FISMA reviews.
- The POA&Ms were not properly updated and provided to the CIO on a quarterly basis.
- The POA&Ms did not contain all elements required by OMB, including details of the estimated resource requirements and corrective action plans to close the POA&M deficiencies. Also, changes to milestones for actions had not been completed.

OMB Memorandum M-08-21¹⁵ states:

POA&Ms must . . . include all security weaknesses found during any other review done by, for, or on behalf of the agency, including [Government Accountability Office] audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.

OMB Memorandum M-08-21¹⁶ further states:

¹⁵ OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 14, 2008.

¹⁶ Ibid.

A [POA&M], also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

OMB Memorandum M-02-01¹⁷ provides the required elements and procedures for the POA&M process.

An IBWC official stated that the policy and procedures had not been approved by management and were still in draft form. Without periodic updates and reviews of POA&M activities, IBWC management may be unaware of the statuses of corrective actions. As a result, delays in the implementation of corrective actions may not be appropriately identified and resolved in a timely manner.

Recommendation 8. OIG recommends the Chief Information Officer implement a Plan of Action and Milestones (POA&M) process and review the quarterly POA&M reports and all elements of the POA&M, as required by Office of Management and Budget Memorandums M-02-01 and M-08-21.

Management Response: IBWC concurred with the recommendation, stating that the draft POA&M “policy and procedure, which includes controls to methodically address findings and facilitate review by the CIO on a quarterly basis is currently being reviewed by management for approval by the Commissioner.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented a POA&M process and has reviewed the quarterly POA&M reports and all elements of the POA&M.

F. Remote Access

IBWC had not developed and implemented a remote access policy and procedure to comply with NIST requirements. NIST SP 800-53, Revision 3, states that the organization documents, monitors, and controls all methods of remote access (for example, dial-up and the Internet) to the information system, including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

An IBWC official stated that the access control (AC) policy and procedure document contains procedures for remote access. However, OIG noted that the AC procedure did not adequately address the remote access process. Without proper policies and procedures that

¹⁷ OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, Oct. 17, 2001.

require documentation of all requests and authorizations of system access, individuals may introduce vulnerabilities into IBWC's network.

Recommendation 9. OIG recommends that the Chief Information Officer develop a remote access policy and procedure, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Response: IBWC concurred with the recommendation, stating that the IMD "is currently updating the existing Access Control policy and procedure to more adequately document the remote access process."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has developed a remote access policy and procedure.

G. Continuous Monitoring

IBWC had not developed a means to implement continuous monitoring of its information technology systems. OIG found that although IBWC had assessed some of the controls of the operating environment, these were manual controls and IBWC had not performed automated routine security assessments of its system environment using the framework outlined in NIST SP 800-53A.¹⁸ In November 2009, IBWC performed the security test and evaluation to verify compliance with its security policy guidelines and to evaluate the effectiveness of the security controls against anticipated threats. In addition, IBWC ensured that a comprehensive testing activity was identified to cover all appropriate security requirements, involved all necessary individuals, and ultimately provided the information needed to support the security assessment and authorization (formerly the certification and accreditation) process. However, IBWC had not expanded the process to include the periodic re-performance of vulnerability scans for its systems or automated routine performance of such scans on its enterprise network.

NIST SP 800-53, Revision 3,¹⁹ states that the organization "scans for vulnerabilities in the information system [in accordance with organization defined] and when new vulnerabilities potentially affecting the system/application are identified and reported.

NIST SP 800-53, Revision 3,²⁰ states:

The organization subsequently initiates specific follow-on actions as part of a comprehensive continuous monitoring program. The continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment

¹⁸ NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, RA-5 Vulnerability Scanning, July 2008.

¹⁹ NIST SP 800-53, rev. 3, *Monitoring Security Controls*, pg. 27, Aug. 2009.

²⁰ *Ibid.*

of operation (RMF Step 6). In particular, the organization revisits on a regular basis, the risk management activities described in the Risk Management Framework. In addition to the ongoing activities associated with the implementation of the Risk Management Framework, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls. These events include, for example:

- An incident results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
- A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information;
- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system; or
- Significant changes to the organizational risk management strategy, information security policy, supported missions and/or business functions, or information being processed, stored, or transmitted by the information system.

When such events occur, organizations, at a minimum, take the following actions:

- *Reconfirm the security category and impact level of the information system.* The organization reexamines the FIPS 199 security category and FIPS 200 impact level of the information system to confirm that the security category and system impact level previously established and approved by the authorizing official are still valid. The resulting analysis may provide new insights as to the overall importance of the information system in allowing the organization to fulfill its mission/business responsibilities.
- *Assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.* The organization investigates the information system vulnerability (or vulnerabilities) exploited by the threat source (or potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan. The exploitation of information system vulnerabilities by a threat source may be traced to one or more factors including but not limited to: (i) the failure of currently implemented security controls; (ii) missing security controls; (iii) insufficient strength of security controls; and/or (iv) an increase in the capability of the threat source. Using

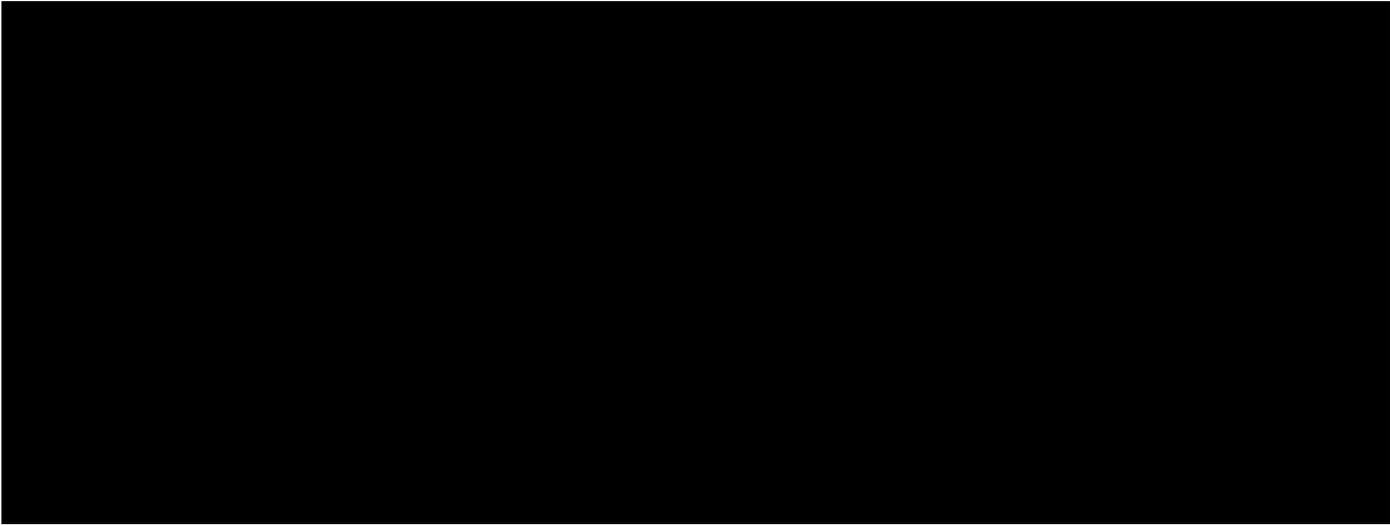
the results from the assessment of the current security state, the organization reassesses the risks arising from use of the information system.

- *Plan for and initiate any necessary corrective actions.*
Based on the results of an updated risk assessment, the organization determines what additional security controls and/or control enhancements or corrective actions for existing controls are necessary to adequately mitigate risk. The security plan for the information system is updated to reflect any initial changes to the original plan. A plan of action and milestones is developed for any noted weaknesses or deficiencies that are not immediately corrected and for the implementation of any security control upgrades or additional controls.

After the security controls and/or control upgrades have been implemented and any other weaknesses or deficiencies corrected, the controls are assessed for effectiveness to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. If necessary, the security plan is updated to reflect any additional corrective actions taken by the organization to mitigate risk.

Additionally, NIST SP 800-53, Revision 3,²¹ states that the risk assessment policy and procedures should include the following:

- a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.



²¹ Ibid.



An IBWC official stated that there is no continuous monitoring program in place that includes routine vulnerability scanning, log monitoring, and notification of unauthorized devices. Also, policies and procedures detailing the strategy and plans for conducting continuous monitoring activities are not documented. Without periodic reviews or the performance of risk-based security assessments, new threats and vulnerabilities may not be identified and mitigated in a timely manner.

Recommendation 10. OIG recommends that the Chief Information Officer develop and implement policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for all major systems and general support systems (GSS). The results of such security assessments should be reviewed, and Plans of Action and Milestones should be developed for the improvement of the security controls of major systems and GSS, as required by National Institute of Standards and Technology Special Publications 800-53, Revision 3, and 800-53A.

Management Response: IBWC concurred with the recommendation, stating that the IMD “has acquired hardware and software that will provide the necessary tools to establish an effective continuous monitoring program.” IBWC also stated the IMD had “installed a Solar Winds Orion network performance monitor that will grant them the ability to monitor network activity.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has developed and implemented policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for all major systems and GSSs.

H. Contingency Planning

IBWC’s COOP does not comply with NIST SP 800-34.²⁴ Specifically, IBWC had not updated its contingency plan and testing policies and procedures. Specifically, the IBWC COOP for its GSS had not been updated to reflect significant changes to the environment, and testing had not been performed.

NIST SP 800-34, Revision 1,²⁵ states that information systems are “vital elements” in most business functions and that “it is critical” that the services provided by these systems be able to operate effectively without excessive interruption. The publication further states, “Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.”

An IBWC official stated that the field offices in Nogales, San Diego, and Yuma (AZ) are configured for a manual backup process and that the manual backup is performed remotely on a monthly basis. The data is backed up on an on-site Terabyte external drive. There is no off-site

²⁴ NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

²⁵ Ibid.

backup for the three field offices. NIST SP 800-53, Revision 3,²⁶ requires agencies to identify an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards and to conduct annual tests of backup information to verify media reliability and information integrity.

An IBWC official stated that the COOP needs to be reassessed and that there was a manual backup process because of the types of servers at the sites. Also, although an alternate site is running, its status as a “hot” or “cold” site²⁷ still needs to be determined. However, the lack of an updated contingency plan may prevent IBWC from accessing critical information and resources and resuming business functions if an extended outage and/or a disaster occurs.

Recommendation 11. OIG recommends that the International Boundary and Water Commission finalize the Continuity of Operations site and conduct testing for operational effectiveness, as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Management Response: IBWC concurred with the recommendation, stating that the IMD “is in the process of updating the current COOP policy and procedure as the infrastructure at the COOP site in Las Cruces, NM continues to be developed.” IBWC also stated that the IMD “is developing a continuity plan to be reviewed by management to determine what level of COOP the IMD will be required to maintain, taking into consideration the financial and maintenance requirements needed.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has finalized the Continuity of Operations site and conducted testing for operational effectiveness.

Recommendation 12. OIG recommends that the International Boundary and Water Commission identify an off-site backup for its field offices in Nogales (AZ), San Diego (CA), and Yuma (AZ), as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Management Response: IBWC stated that the recommendation is resolved in that the IMD “has acquired the needed client to allow for the full offsite backup of all field offices.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has identified an off-site backup for the three field offices specified.

²⁶ NIST SP 800-53, rev. 3, Aug. 2009.

²⁷ A hot site is a building already equipped with processing capability and other services, and a cold site houses processors that can be easily adapted for use.

I. Oversight of Contractor System

IBWC had not implemented an effective oversight program of its contractor system.

Since IBWC had not developed policies and procedures to oversee the San Diego operations, the field office relied heavily on contractor-produced policies and procedures.

OIG also found that IBWC officials did not have adequate control over the IT functions at the San Diego waste treatment plant or the IT assets purchased and maintained by the contractor in support of operations. During its fieldwork, OIG found that the contractor had an inappropriate degree of latitude on purchases of IT assets, with little or no input from IBWC management. Additionally, contractor-owned software was operating on the local area network (LAN) at the San Diego waste treatment plant without proper review and approval by IBWC's IMD.

OMB Memorandum M-11-33³⁰ states: "Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems."

An IBWC official stated that the inventory database had not been updated to remove old components or include newly purchased components. The San Diego Field Office project manager's understanding was that oversight of contractor operations was assigned to the field office and the contracting officer's representative and that the IT functions rest with IMD. However, the contracting officer's representative is responsible more specifically for the employees and for hardware/operations of the plant rather than for the IT assets. Without adequate contractor oversight, IBWC has minimal assurance that contractor personnel are compliant with FISMA, OMB requirements, and NIST standards. Further, because the IMD has no review and approval process, contractors may be purchasing IT assets that are not in the best interest of IBWC. Finally, without proper oversight, there is an increased risk that data collected, processed, and maintained is exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

Recommendation 13. OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is involved in the oversight of information technology assets purchased and maintained by the contractor in

³⁰ OMB Memorandum M-11-33, Sept. 14, 2011.

support of operations at the waste treatment plant in San Diego (CA), as required by National Institute of Standards and Technology Special Publications 800-53, Revision 3, and 800-82 and with Office of Management and Budget Memorandum M-11-33.

Management Response: IBWC concurred with the recommendation, stating that the CIO “is requiring modifications to the contract in place, to ensure the IMD is notified in a timely manner, of all planned technology asset purchases, in order to provide the required level of oversight of new IT purchases and existing assets maintained by the contractor.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented oversight of IT assets purchased and maintained by the contractor in support of operations at the waste treatment plant in San Diego.

Recommendation 14. OIG recommends that the International Boundary and Water Commission (IBWC) ensure that its Information Management Division reviews and approves software prior to installation on IBWC assets, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and Office of Management and Budget Memorandum M-11-33.

Management Response: IBWC concurred with the recommendation, stating that the CIO “is requiring modifications to the contract in place, to ensure the IMD is notified in a timely manner of all planned software purchases in order to provide the required level of oversight of new IT purchases and existing software maintained by the contractor.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented a process to review and approve software prior to installation on IBWC assets.

J. Security Capital Planning

Information security is not integrated into IBWC’s Capital Planning and Investment Control process. IBWC did not provide OMB with a detailed explanation for the major investment related to its IT capital investment. Inadequate planning increases the risk that requests for funding investments will not receive proper consideration. An IBWC official stated that the resource management goals within the IBWC strategic plan did not include IT. According to IBWC officials, because IBWC is a small organization, its budget requirements are not at the level established for reporting to OMB. IBWC understands the threshold to be \$2 million, but IBWC current IT assets are approximately \$100,000. However, IBWC acknowledged that the current assets do not include the SCADA systems. As such, IBWC had been using the IT workplan and had not been assessing the risk identified in the POA&Ms as part of the IBWC capital planning request. IBWC has been working on a year-to-year IT workplan to identify high priority tasks to continue developing the IT environment.

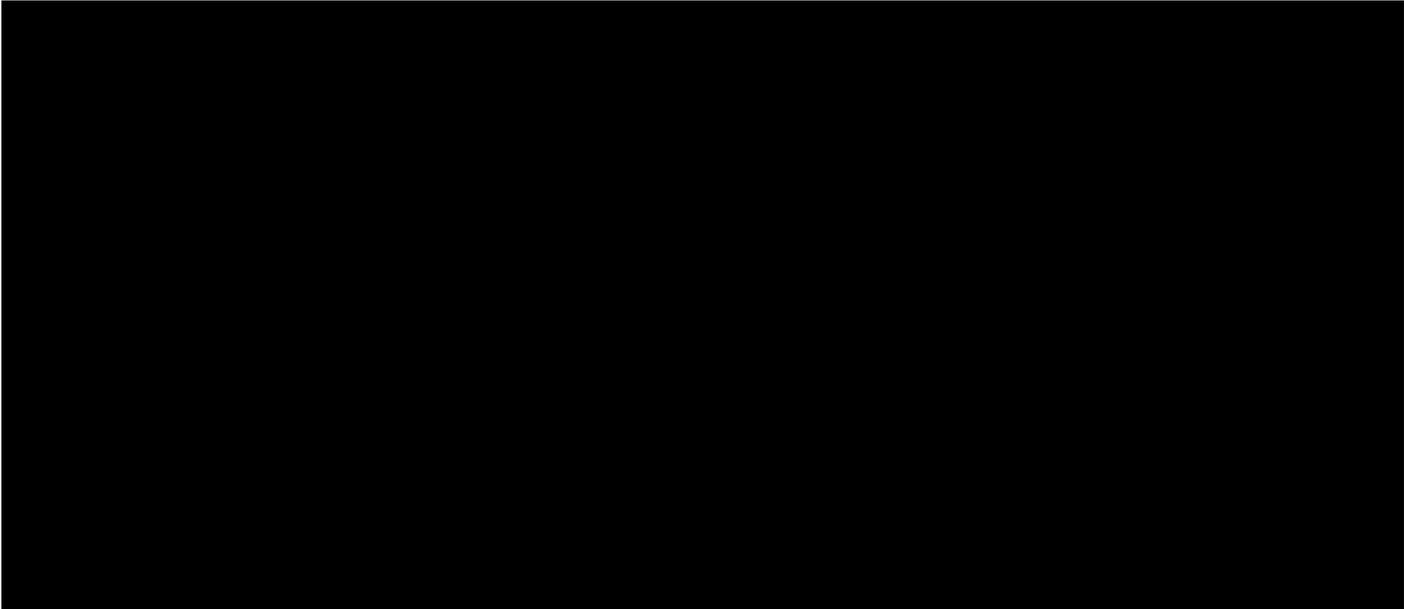
OMB Memorandum M-11-33³¹ mandates that IBWC “integrate and fund IT security over the life cycle of each system.” The memorandum also states that security requirements for a steady-state (existing) system (including maintenance and operation costs at its current capability and performance level) must be met before spending funds on new systems or modernizing an existing system.

The lack of integration between the POA&M process and the capital planning process negatively affects the funding prioritization in IBWC. The current process does not properly consider needed IT investments and subsequently fails to request necessary funding.

Recommendation 15. OIG recommends that the Chief Information Officer ensure that all funding for information technology (IT) security investments and IT components is tracked, as required by Office of Management and Budget Memorandum M-11-33.

Management Response: IBWC concurred with the recommendation, stating that the CIO “will utilize and expand upon the existing budget account structure in place to track all expenses by Operating Allowance or Cost Center for all labor and non-labor costs to track all IT costs.” IBWC also stated that it “will ensure that through an effective information security program” that IBWC “will effectively protect information and systems as well as maintain the integrity, reliability, availability, and confidentiality of our information, consistent with Office of Management and Budget Memorandum M-00-07 and M-06-19.”

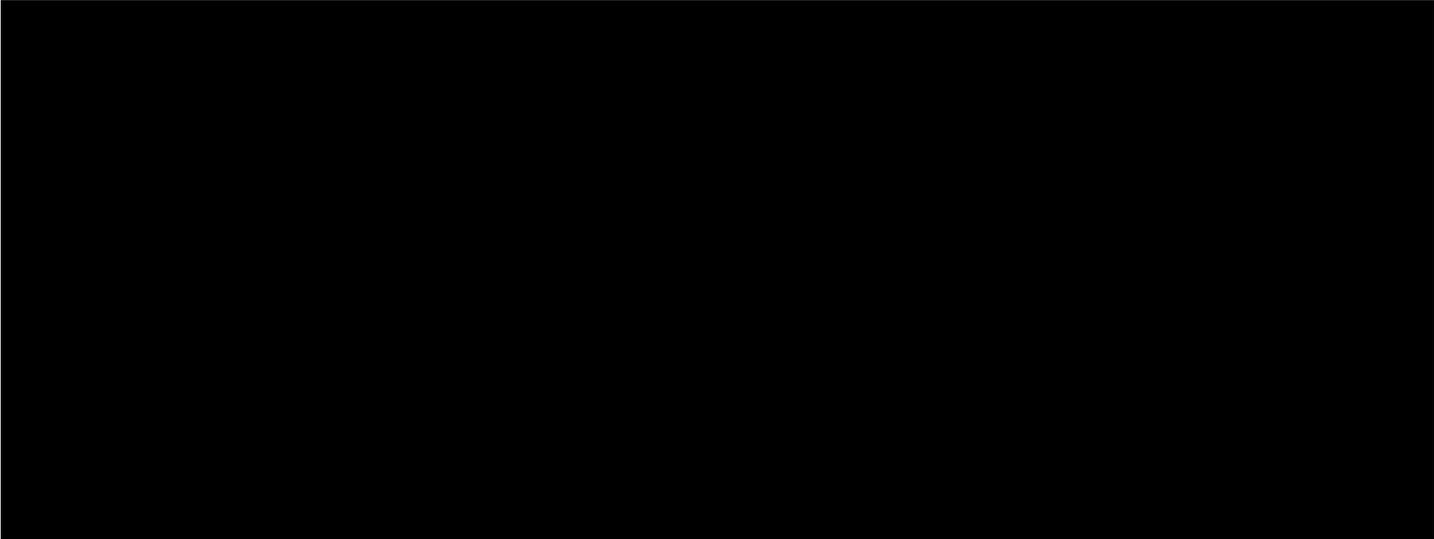
OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has ensured that all funding for IT security investments and IT components is tracked.



³¹ OMB Memorandum M-11-33, Sept. 14, 2011.

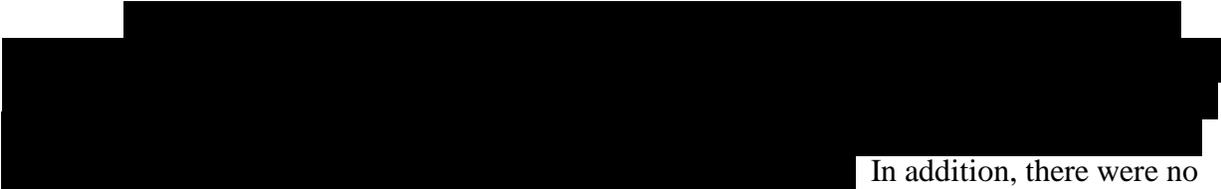


~~SENSITIVE BUT UNCLASSIFIED~~



In addition to the weakness in physical and environmental protection already mentioned, OIG identified a weakness with physical access to the server room at IBWC's United States Section headquarters in El Paso. Access is not granted on a "need to know" basis; rather, all IMD staff members have access. The server room is accessed through a locked door with a cipher lock; however, employees do not have unique combinations (all employees use the same combination for access), and this defeats the accountability and control to IBWC's information and information systems.

According to NIST SP 800-53, Revision 3,³³ the organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible), issues authorization credentials, reviews and approves the access list and authorization credentials, and removes from the access list personnel no longer requiring access.



In addition, there were no emergency shutoffs of power or emergency lighting within the computer area to prevent damage to equipment or injury to personnel. Finally, IBWC had not maintained fire suppression and detection devices for water and humidity.

NIST SP 800-53, Revision 3,³⁴ states that "the organization protects power equipment and power cabling for the information system from damage and destruction." NIST SP 800-53 also states that "the organization provides the capability to shut off power to the information system or individual system components in emergencies; provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a

³³ NIST SP 800-53, rev. 3, PE-2 Physical Access Authorizations, Aug. 2009.

³⁴ Ibid, PE-9 Power Equipment and Power Cabling, PE-10 Emergency Shutoff, PE-11 Emergency Power, PE-12 Emergency Lighting, and PE-13 Fire Protection apply.

~~SENSITIVE BUT UNCLASSIFIED~~

primary power source loss; employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility; and employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.”

Without an effective physical and environmental protection plan, personnel may be unaware of risks that could compromise the confidentiality, integrity, and availability of data or result in injuries to personnel and damage or destruction of IBWC IT assets.



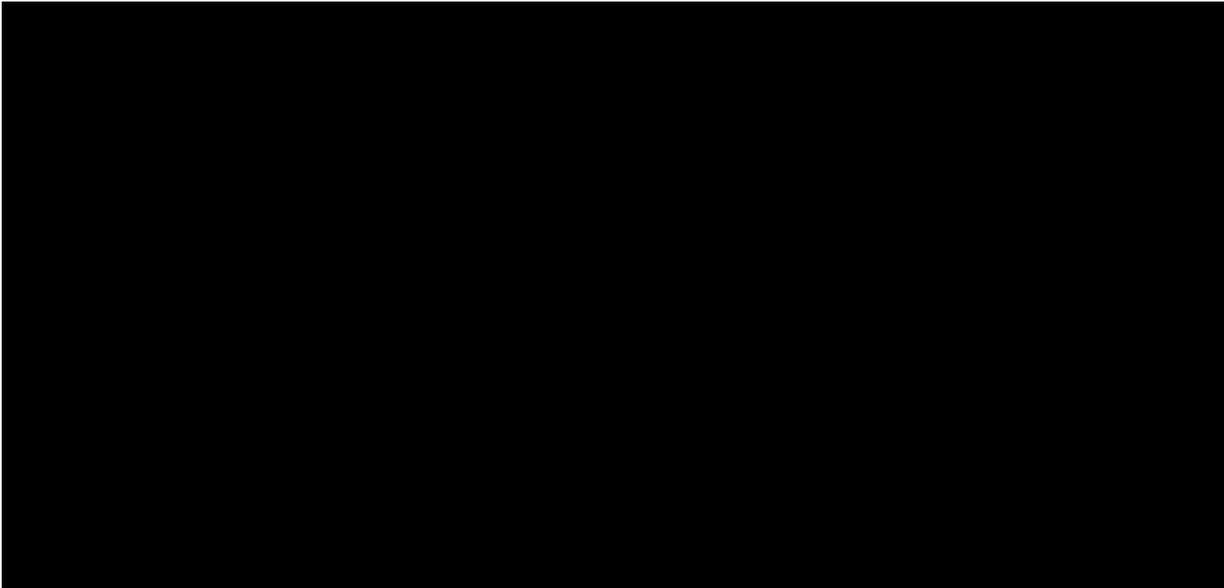
Recommendation 19. OIG recommends that the International Boundary and Water Commission implement a process to review, update, and approve the Information Management Division staff access list to the server room at its office in El Paso (TX), as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Response: IBWC concurred with the recommendation, stating that the CIO and the IMD recognize “the risks associated with an unmonitored entry way into the agency’s main LAN [local area network] room and will take the necessary steps to implement an additional proximity card reader to limit access to only authorized IMD personnel.”

~~SENSITIVE BUT UNCLASSIFIED~~

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented a process to review, update, and approve IMD's staff access list to the server room at its office in El Paso.

Recommendation 20:



Recommendation 21. OIG recommends that the International Boundary and Water Commission determine the most cost-effective protective measures for fire prevention and damage to file servers, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Response: IBWC concurred with the recommendation, stating that the CIO "is working with the IMD to issue specific guidance to the San Diego and Yuma Area Operations Managers, detailing actions required removing all unnecessary items out of the server rooms to minimize or eliminate the potential of damage to equipment or injury to personnel."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that IBWC has implemented the most cost-effective protective measures for fire prevention and damage to file servers.

~~SENSITIVE BUT UNCLASSIFIED~~

List of Recommendations

Recommendation 1: OIG recommends that the Chief Information Officer ensure that all assets are accounted for in the inventory system and develop a process that updates, not less than annually, the International Boundary and Water Commission's (IBWC) system inventory when changes are made to those information systems operated by or under the control of IBWC or by third-party contractors or agencies on behalf of IBWC, as required by the Federal Information Security Management Act.

Recommendation 2: OIG recommends that the Chief Information Officer improve the risk management strategy at the organizational level for assessing, responding to, and monitoring information security risk, as required in National Institute of Standards and Technology Special Publication 800-37, Revision 1.

Recommendation 3: OIG recommends that the Chief Information Officer:

- Develop the security assessment and authorization packages for the Supervisory Control and Data Acquisition systems as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-82 and NIST SP 800-53, Revision 3.
- Improve existing procedures to ensure security assessment and authorization packages are updated every 3 years or when a significant change occurs, as required by NIST SP 800-37, Revision 1.
- Improve existing procedures to ensure system security plans and security assessment reports are updated as required to comply with the security baseline controls in NIST SP 800-53, Revision 3.
- Perform annual security assessments of a subset of a system's security controls, as required by NIST SP 800-37, Revision 1.

Recommendation 4: OIG recommends the Chief Information Officer develop and implement security configuration management procedures and periodically assess compliance with the implemented procedures, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 5: OIG recommends that the Chief Information Officer develop procedures for the oversight of all systems and hardware that are part of the International Boundary and Water Commission operations, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 6: OIG recommends that the Chief Information Officer enforce the security awareness training policy requiring all personnel to attend initial and refresher security awareness training and enforce consequences of non-compliance for personnel who do not successfully complete the security awareness training, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3, and Office of Management and Budget Circular No. A-130.

Recommendation 7: OIG recommends that the Chief Information Officer enforce the security awareness training requirement for those personnel with significant security responsibilities, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3, and Office of Management and Budget Circular No. A-130.

Recommendation 8: OIG recommends the Chief Information Officer implement a Plan of Action and Milestones (POA&M) process and review the quarterly POA&M reports and all elements of the POA&M, as required by Office of Management and Budget (OMB) Memorandums M-02-01 and M-08-21.

Recommendation 9: OIG recommends that the Chief Information Officer develop a remote access policy and procedure, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3.

Recommendation 10: OIG recommends that the Chief Information Officer develop and implement policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for all major systems and general support systems (GSS). The results of such security assessments should be reviewed, and Plans of Action and Milestones should be developed for the improvement of the security controls of major systems and GSS, as required by National Institute of Standards and Technology Special Publications 800-53, Revision 3, and 800-53A.

Recommendation 11: OIG recommends that the International Boundary and Water Commission finalize the Continuity of Operations site and conduct testing for operational effectiveness, as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

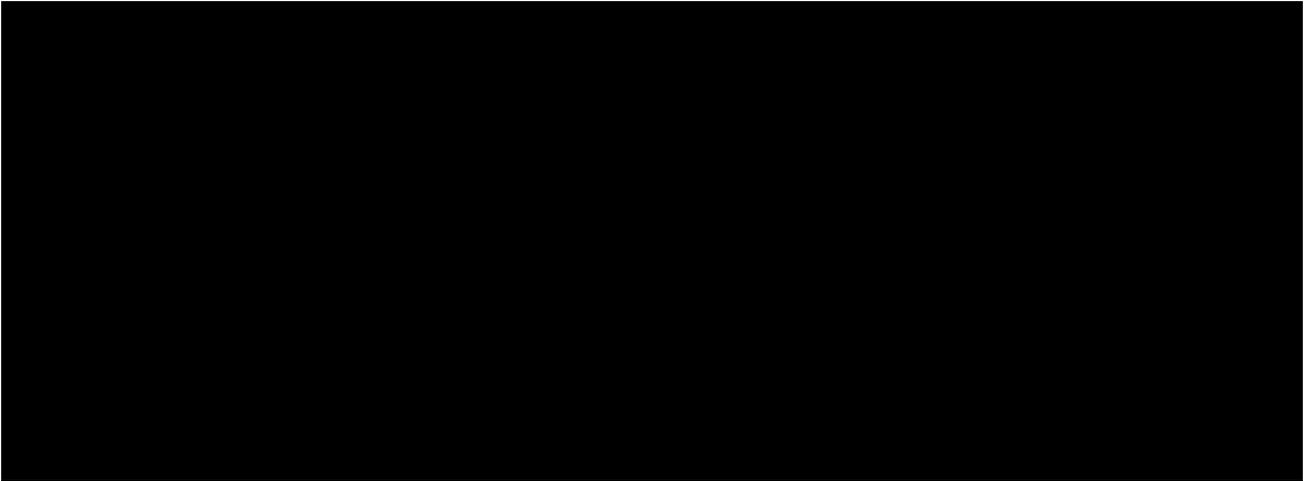
Recommendation 12: OIG recommends that the International Boundary and Water Commission identify an off-site backup for its field offices in Nogales, (AZ), San Diego (CA), and Yuma (AZ), as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Recommendation 13: OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is involved in the oversight of information technology assets purchased and maintained by the contractor in support of operations at the waste treatment plant in San Diego (CA), as required by National Institute of Standards and Technology Special Publications 800-53, Revision 3, and 800-82 and with Office of Management and Budget Memorandum M-11-33.

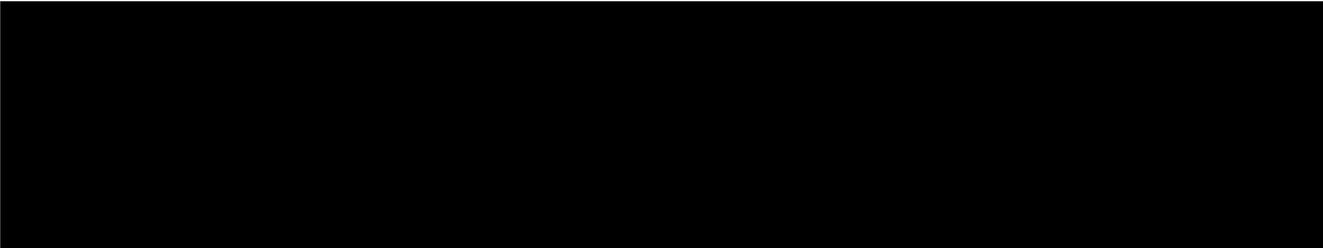
Recommendation 14: OIG recommends that International Boundary and Water Commission (IBWC) ensure that its Information Management Division reviews and approves software prior to installation on IBWC assets, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and Office of Management and Budget Memorandum M-11-33.

~~SENSITIVE BUT UNCLASSIFIED~~

Recommendation 15: OIG recommends that the Chief Information Officer ensure that all funding for information technology (IT) security investments and IT components is tracked as required by Office of Management and Budget Memorandum M-11-33.



Recommendation 19: OIG recommends that the International Boundary and Water Commission implement a process to review, update, and approve the Information Management Division staff access list to the server room at its office in El Paso (TX), as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.



Recommendation 21: OIG recommends that the International Boundary and Water Commission determine the most cost-effective protective measures for fire prevention and damage to file servers, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~SENSITIVE BUT UNCLASSIFIED~~

Appendix A. Objectives, Scope, and Methodology

To fulfill its responsibilities related to the Federal Information Security Management Act of 2002 (FISMA), the Office of Inspector General (OIG), Office of Audits, visited the El Paso (TX) headquarters and the San Diego (CA) and Yuma (AZ) field operations offices to evaluate the International Boundary and Water Commission's (IBWC) information technology security program and practices and to determine the effectiveness of the program for FY 2011.

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency's inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

OIG conducted its evaluation from June through October 2011. In addition, OIG performed the evaluation in accordance with generally accepted government auditing standards (GAGAS) and with FISMA, OMB, and National Institute of Standards and Technology Special Publication guidance. GAGAS requires the audit to be planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. OIG believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objectives.

OIG performed fieldwork from July through October 2011. The fieldwork was completed before OMB Memorandum M-11-33, dated September 14, 2011, which provided instructions for FY 2011 reporting requirements,¹ was issued. OIG reviewed the memorandum and evaluated its impact on the results of the evaluation but determined that no changes were required.

¹ OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated Sept. 14, 2011.

Appendix B. Followup of Recommendation From the FY 2010 Federal Information Security Management Act Report

The FY 2010 Federal Information Security Management Act (FISMA) evaluation was conducted by an independent public accounting firm, which issued its report (*Audit of the International Boundary and Water Commission Federal Information Security Management Act* issued July 30, 2010) with one consolidated finding and recommendation. The evaluation team reviewed actions implemented by management to respond to the findings identified in the FY 2010 FISMA report.

FY 2010 FISMA Recommendation

We recommend that USIBWC management continue its efforts to ensure that its information security program complies with the standards and guidelines established by NIST and OMB.

The status of the recommendation as presented in the report:

2011 Status: Closed. OIG reviewed the findings related to the recommendation and noted that all findings were lumped into one recommendation. However, OIG separated each finding and assigned separate recommendations in the FY2011 FISMA evaluation to provide IBWC management the ability to close the recommendation as corrective action is completed rather than waiting until all of identified components of the recommendation are corrected.

Appendix C. OIG Outline for Action: Physical Security Concerns at the International Boundary and Water Commission



United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

AUG 26 2011

The Honorable Edward Drusina, U. S. Commissioner
International Boundary and Water Commission
United States and Mexico, U.S. Section
4171 North Mesa Street, Suite C-100
El Paso, TX 79902-1441

Dear Commissioner ~~Drusina~~:

In accordance with the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347, Title III), the Department of State, Office of Inspector General (OIG), recently conducted a review of the International Boundary and Water Commission's (IBWC) information security program and practices. The objective of this review was to evaluate the progress IBWC has made in implementing an effective information security program and related practices.

OIG's Office of Audits performed the review at the El Paso (TX) headquarters and at the Yuma (AZ) and San Diego (CA) field operations offices. The complete results of the review will be issued in the FY 2011 IBWC FISMA report. However, during its review, OIG identified two physical security concerns that require your immediate attention: lack of completion of background investigations of employees and contractors at IBWC and lack of control procedures over the remote gate devices and access to IBWC operations in San Diego. The findings and recommendations are outlined in the enclosed OIG Outline for Action.

Although these recommendations will be included in OIG's FY 2011 IBWC FISMA report, immediate action is needed to address these security issues. Therefore, please provide a response to the recommendations within 10 days of the date of this correspondence.

If you have any questions, please contact Evelyn R. Klemstine, Assistant Inspector General for Audits, by email at klemstinee@state.gov or at (202) 663-0372 or Jerry Rainwaters, Information Technology Division Director, by email at rainwatersj@state.gov or at (703) 284-1841.

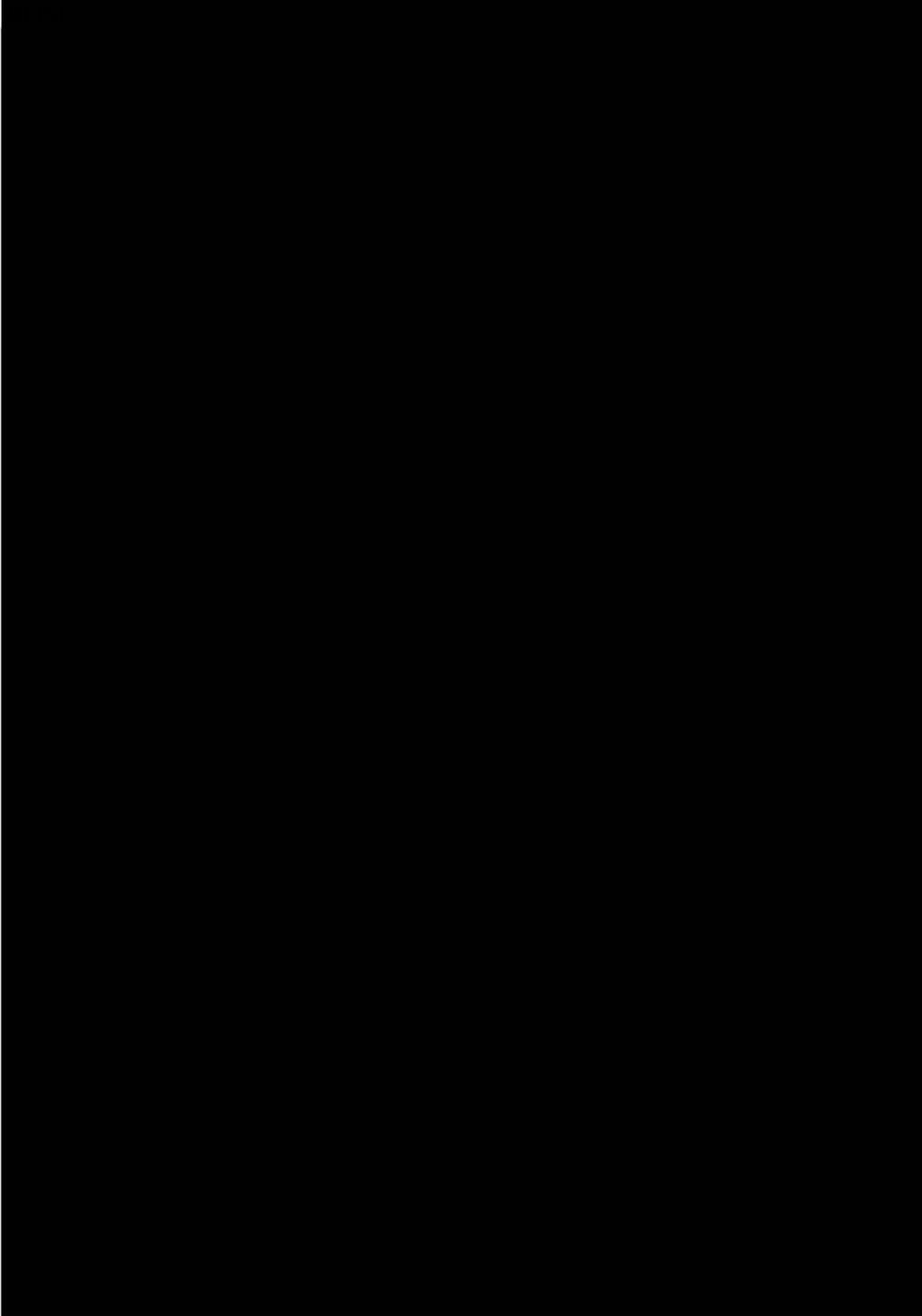
Sincerely,

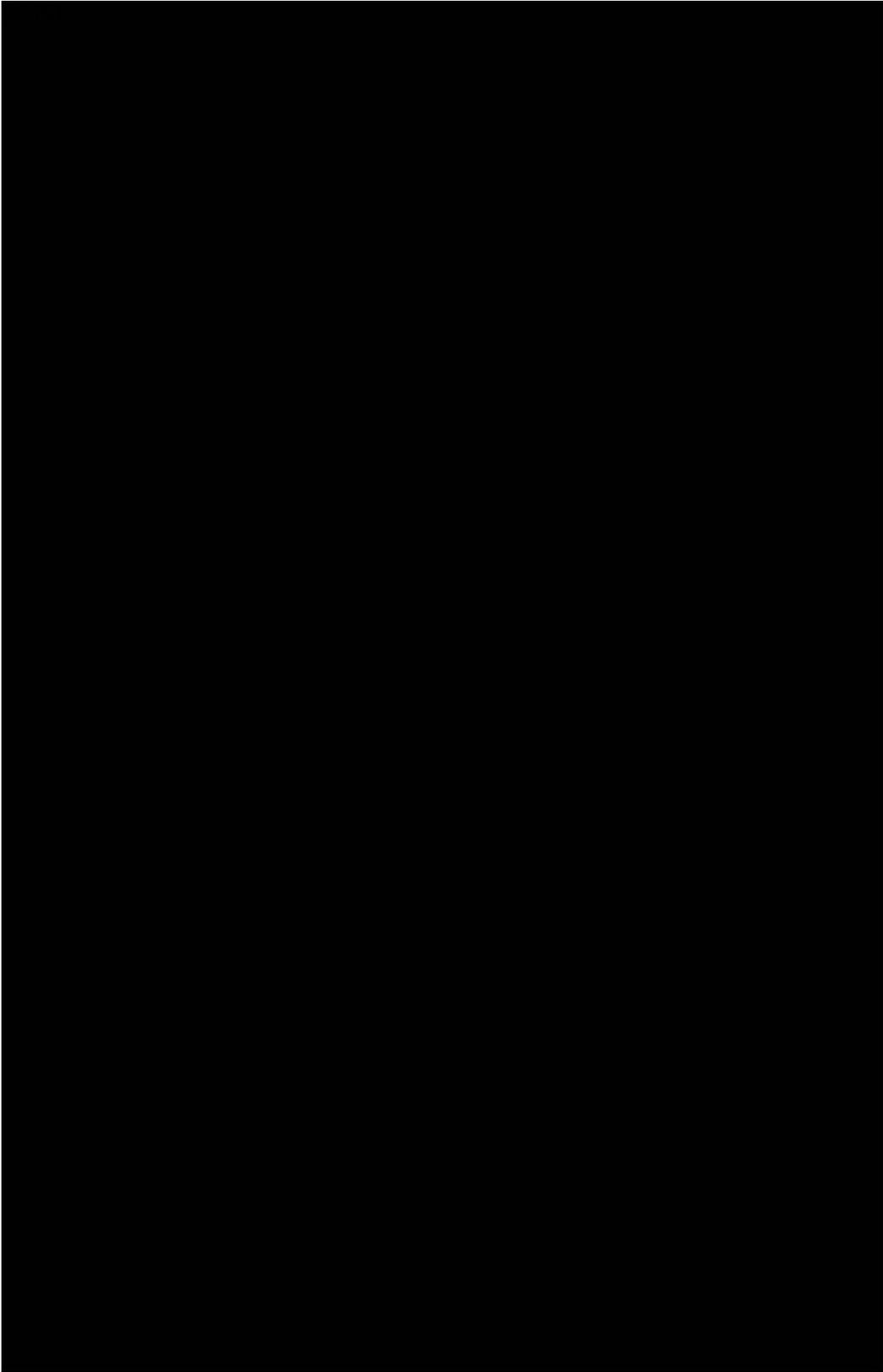
Harold W. Geisel
Deputy Inspector General

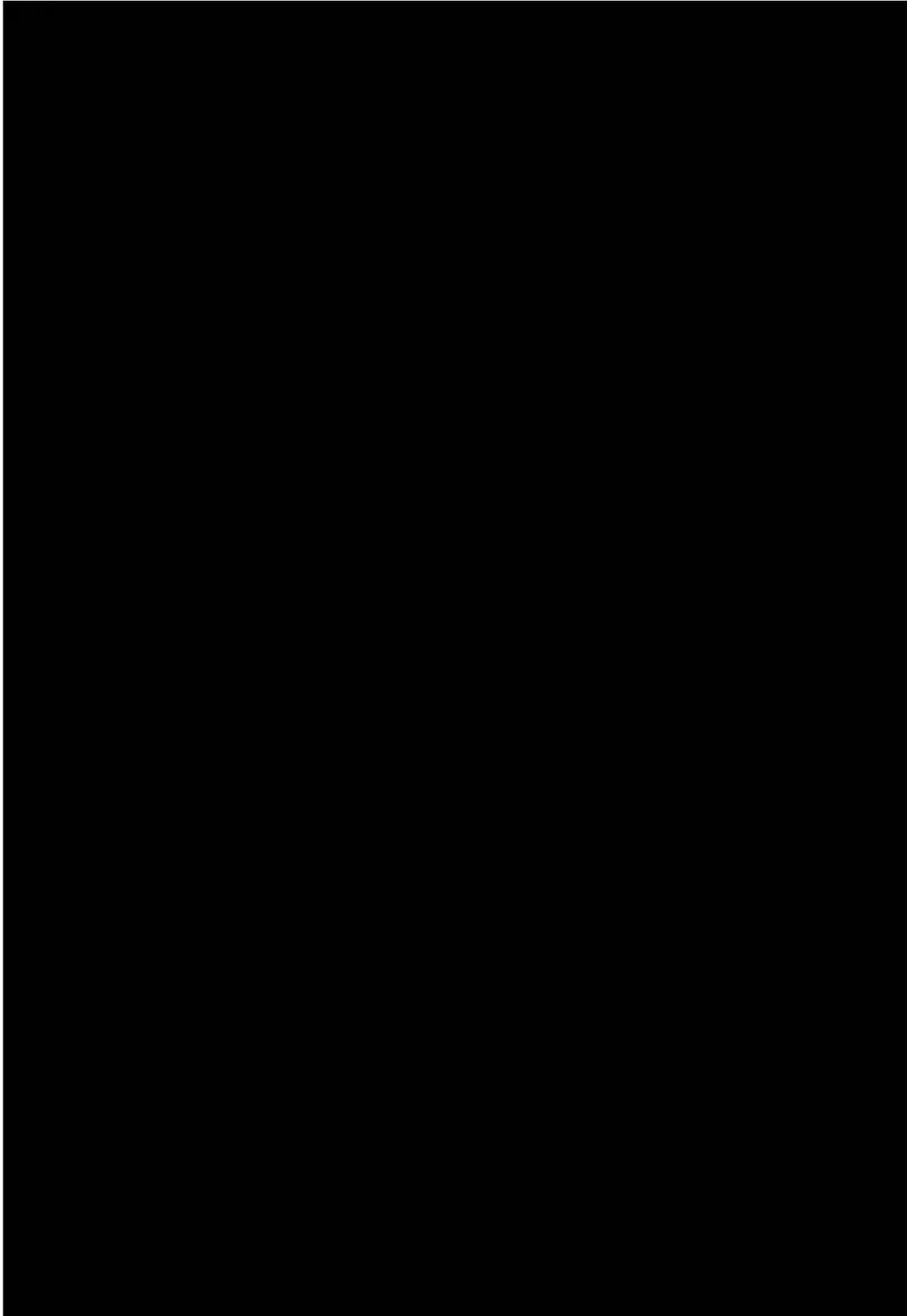
Enclosure

cc: USIBWBC - [REDACTED]
WHA/MEX - [REDACTED]

~~SENSITIVE BUT UNCLASSIFIED~~
DRAFT







Appendix D. International Boundary and Water Commission Response to OIG Outline for Action

INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

September 2, 2011



OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

United States Department of State
Harold W. Geisel
Deputy Inspector General
Office of Inspector General
Washington, D. C. 20520

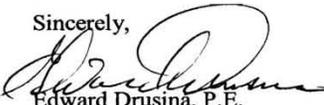
Subject: OIG Outline for Action: Physical Security Concerns at the International Boundary and Water Commission (IBWC)

Dear Mr. Geisel,

Thank you for the opportunity to respond to findings and recommendations reported in the OIG Outline for Action: Physical Security Concerns at the International Boundary and Water Commission report, identified during the conduct of the Federal Information Security Management (FISMA) of 2002 (Public Law 107-347, Title III) review dated August 26, 2011.

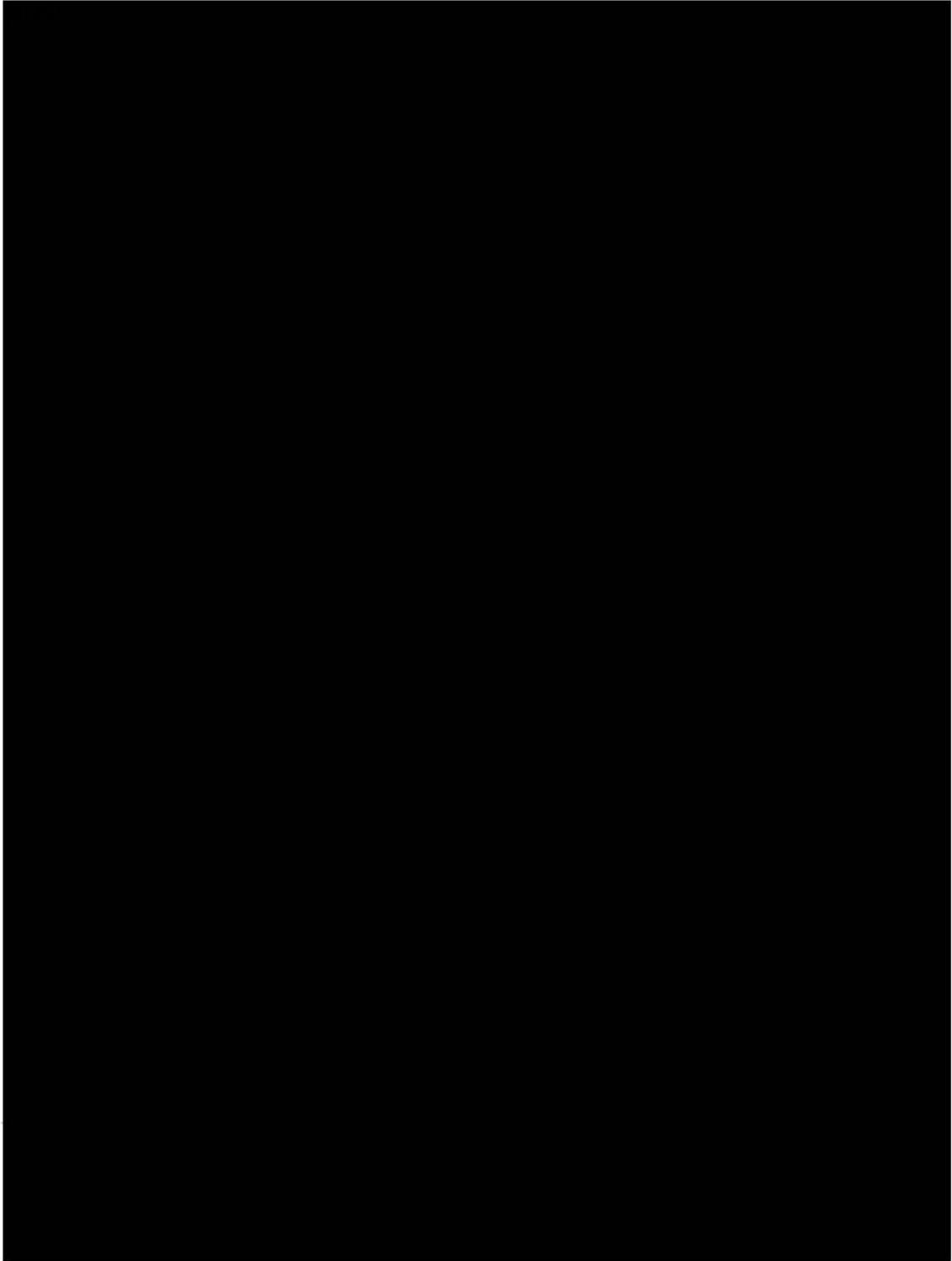
We are pleased to report that immediate steps have been initiated to implement actions to respond to findings and recommendations identified. Specific details for each finding and recommendation are provided attached.

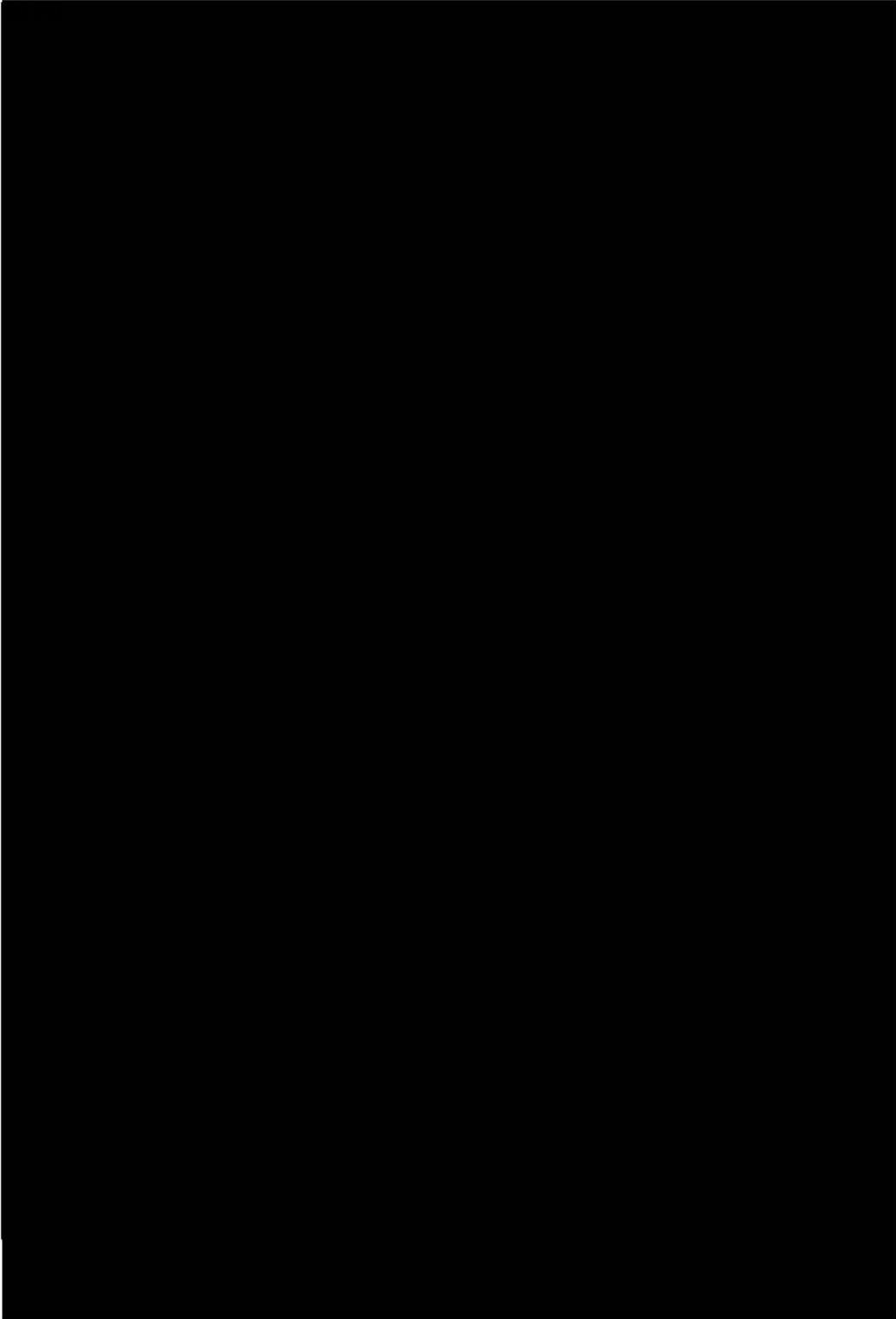
Sincerely,

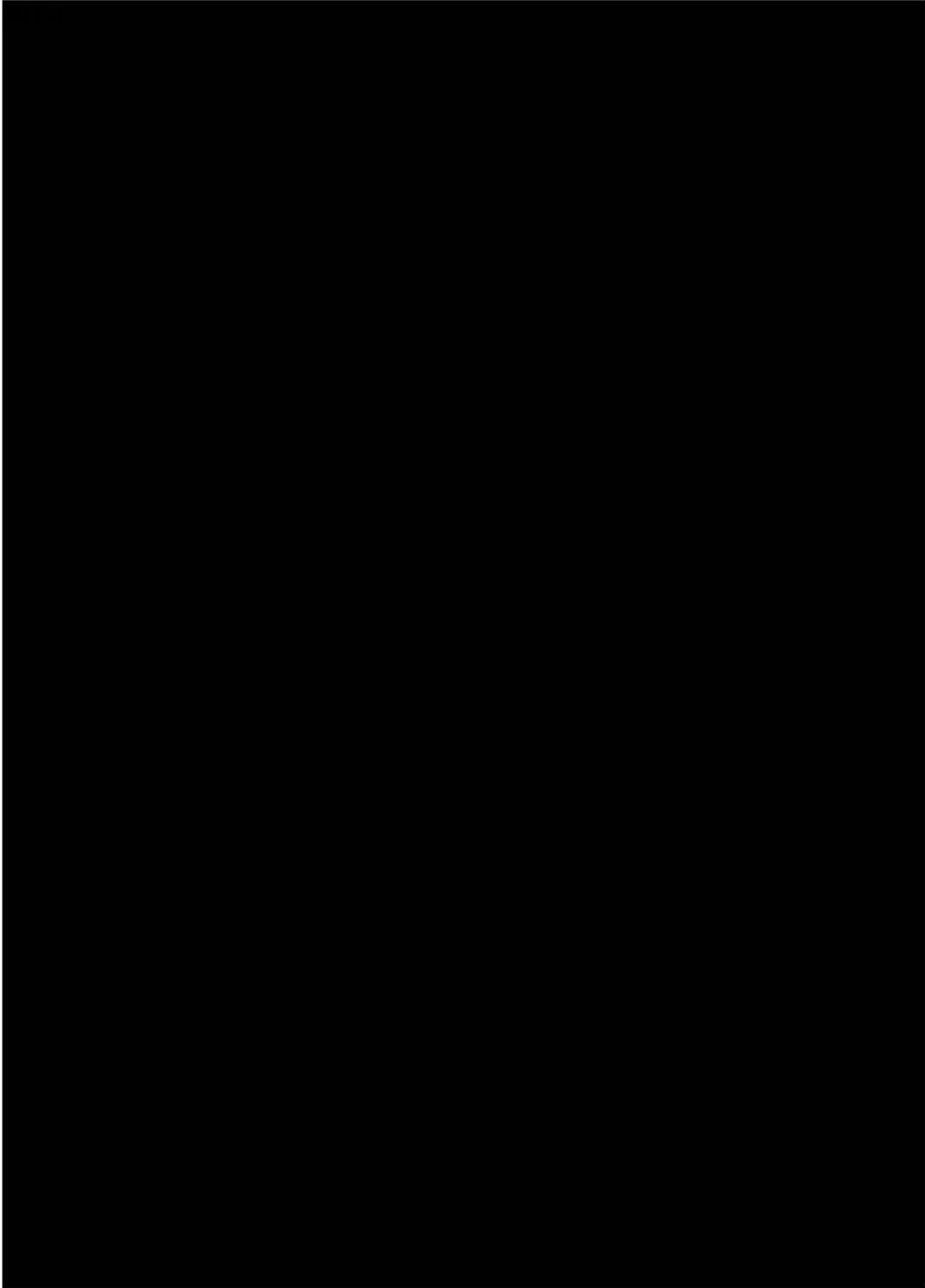


Edward Drusina, P.E.
Commissioner

The Commons, Building C, Suite 100 • 4171 N. Mesa Street • El Paso, Texas 79902-1441
(915) 832-4100 • Fax: (915) 832-4190 • <http://www.ibwc.gov>









Appendix E. International Boundary and Water Commission Response



OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

November 9, 2011

Mr. Harold W. Geisel
United States Department of State
Deputy Inspector General
Office of Inspector General
Washington, D. C. 20520

Subject: Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program

Dear Mr. Geisel:

Thank you for the opportunity to review and comment on the draft report and recommendations. The IBWC is eager to fulfill its responsibilities related to compliance with the Federal Information Security Management Act, and this evaluation has provided us clear objectives towards achieving that goal.

We are pleased to submit the following responses for your review and consideration for inclusion in the final report. Specific details for each finding and recommendation are provided in the attached.

Sincerely,



Edward Drusina, P.E.
Commissioner

The Commons, Building C, Suite 100 • 4171 N. Mesa Street • El Paso, Texas 79902-1441
(915) 832-4100 • Fax: (915) 832-4190 • <http://www.ibwc.gov>

Control Weakness A: System Inventory – IBWC has not implemented a process or procedure to update and manage its information technology (IT) assets. Without a process to properly identify, document and maintain an inventory of systems, IBWC may not have an accurate accounting of all IT assets and related system interfaces and underlying support systems.

Recommendation 1: "OIG recommends that the CIO ensure that all assets are accounted for in the inventory system and develop a process that updates, not less than annually, the IBWC's system inventory when changes are made to those information systems operated by or under the control of IBWC, or by third party contractors or agencies on behalf of IBWC as required by the federal Information Security Management Act"

Response/Action: Concur. The Information Management Division has initiated the development of its own IT asset inventory, in addition to the one maintained within the Department of State Integrated Logistics Management System (ILMS), in order to accurately account for all IT assets that make up the General Support System and existing Supervisory Control and Data Acquisition (SCADA) systems identified in San Diego, CA, Nogales, AZ, Amistad and Falcon, TX. Current system inventory documentation and the existing System Security Plan (SSP) are being updated to include the identified SCADA systems and the assets identified in the 1st and 3rd floor wiring closets. The existing SSP is also being updated to identify the interfaces between the Headquarters and field office LANs, and to document other networks not operated by the agency. All scheduled field office visits by the IMD will include a thorough inventory of all IT assets and documentation of their locations. Newly developed Configuration Management documentation, particularly system architecture changes that involve the addition of a new configuration item, will contain a method of requiring that the system inventory and related documentation be updated upon full implementation. The existing contract with contractors that operate systems under the IBWC's control is in the process of being modified to require that acquisition of new assets be accounted for and approved by the Information Management Division (IMD) and call for an annual inventory.

Control Weakness B: Risk Management Program - IBWC's risk management program for information security needs improvement at the organization and system levels. At the organizational level, IBWC had not implemented a risk management framework and information security policies and procedures that describe the roles and responsibilities of key participants. OIG found that IBWC did not have procedures for the risk management framework or information security policies and procedures that describe the roles and responsibilities of key participants. As such, OIG could not review the risk management framework and how IBWC manages information security risk..

Recommendation 2: "OIG recommends that the Chief Information Officer improve the risk management strategy at the organizational level for assessing, responding to, and monitoring information security risk as required in National Institute of Standards and Technology Special Publication 800-37 Revision I."

Response/Action: Concur. The CIO has initiated steps necessary to bring about an effective risk management framework and policies and procedures in accordance with NIST SP 800-37 Revision 1. The IMD has begun updating the existing System Security Plan to include all current security baseline controls, changes in the GSS and identified SCADA systems. The IMD will prepare a new security assessment and authorization package to apply for and achieve an Authority to Operate designation from the new Designated Authority in FY12. Following training of two IT Specialists on SCADA

security in November, a security assessment and authorization packages will be completed for all identified SCADA systems.

Recommendation 3: “OIG recommends that the Chief Information Officer:

- Develop the security assessment and authorization packages for the Supervisory Control and Data Acquisition systems as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-82 and NIST SP 800-53, Revision 3.
- Improve existing procedures to ensure security assessment and authorization packages are updated every 3 years or when a significant change occurs, as required by NIST SP 800-37, Revision 1.
- Improve existing procedures to ensure system security plans and security assessment reports are updated as required to comply with the security baseline controls in NIST SP 800-53, Revision 3.
- Perform annual security assessments of a subset of a system’s security controls as required by NIST SP 800-37, Revision 1.

Response/Action: Concur. The CIO will take all necessary action to comply with all items under this recommendation and to comply with NIST SP 800-53, Revision 3, NIST SP 800-37, Revision 1, and SP 800-82.

Control Weakness C: Configuration Management - IBWC had not implemented effective configuration management (CM) standards and procedures for its IT environment. Although IBWC had CM standards and procedures in place, it did not account for the patch management process to evaluate patches for applicability, installation process, monitoring, and periodic review of the patch status on the systems. Further, IBWC did not maintain control over all hardware connected to its SCADA system in San Diego.

Recommendation 4: “OIG recommends the Chief Information Officer develop and implement security configuration management procedures and periodically assess compliance with the implemented procedures as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.”

Response/Action: Concur. The draft Configuration Management policy and procedure is currently being reviewed by management for approval by the Commissioner. The CIO has access to the IMD’s collaboration intranet site to allow constant assessments on compliance with the newly implemented procedures. With the acquisition of new security appliances purchased in FY11, the IMD will be able to evaluate patches for applicability, install, monitor and review patch status on all systems in a much more efficient and effective way.

Recommendation 5: “OIG recommends the Chief Information Officer develop procedures for the oversight of all systems and hardware that are part of the International Boundary and Water Commission operations as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.”

Response/Action: Concur. The IMD has acquired hardware and software that will provide the necessary tools to establish an effective continuous monitoring program. These assets will help the IMD detect and measure the effectiveness of security controls applied within the GSS. All acquired items are in the process of being configured and implemented. The IMD has already installed and

configured a monitor in the general area of the IMD that automatically scrolls through the status screens of several critical systems and services in order to keep them monitored in real-time. A software application called "RedLine" which works with the enterprise email system has recently been configured to email IMD staff if any of the necessary services go down, or are showing signs of failure. Additional equipment include an Intrusion Detection System (IDS), Network Admissions Control (NAC) and a Network Scanner which will all provide automated methods of detecting changes within our GSS and notify the IMD of compromised PC's or those that may show irregular activity. With the installation of new switches at HQ's and all field offices, the IMD will gain port level visibility of all IT assets to inform our personnel of any signs of configuration changes or unauthorized activity. The IMD has also recently installed a Solar Winds Orion network performance monitor that has greatly enhanced our ability to monitor network activity. CISCO works has also been installed which sends alerts to IMD staff when certain network activity thresholds have been exceeded or show signs of potentially dangerous activity. A thorough inventory of all hardware connected to the SCADA system in San Diego has been completed. In addition, the contract currently in place for the Government Owned, Contractor Operated site is being modified to ensure control over all assets located at the site is managed by the IBWC. The contractor will also be required to update their internal policy and procedures to designate oversight of all systems and hardware to the IMD.

Control Weakness D: Security Training - Although IBWC's security awareness training program requires all personnel to complete annual security awareness training and users with significant security responsibilities to complete specialized training, OIG found that IBWC employees had not completed their general security awareness training and employees with significant security responsibilities had not completed their specialized training.

Recommendation 6: "OIG recommends the Chief Information Officer enforce the security awareness training policy requiring all personnel to attend initial and refresher security awareness training and enforce consequences of non-compliance for personnel who do not successfully complete the security awareness training as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3, and Office of Management and Budget Circular No. A-130."

Response/Action: Concur. The IMD conducted five IT Security training classes immediately after the OIG visit in August resulting in 235 employees out of 272 completing their annual IT Security training. Ten out of HQ's and 27 from the field offices did not attend the training sessions resulting in approximately 87% completion rate. All employees at HQ's that did not attend training completed their training through alternate means after the September 30th deadline. Employees in the field offices which have not conducted the training have had their accounts disabled until they are able to complete the IT Security course. The IMD is maintaining the required documentation for all training conducted, along with attendance rosters. The IMD has also acquired a cloud based training system that will allow for a much more efficient method to provide IT Security training to IBWC personnel. The new system will establish a username and password for each employee to enter the training and their completion of over twelve modules will be monitored, to include scoring of review questions at the end of each module.

Recommendation 7: "OIG recommends the Chief Information Officer enforce the security awareness training requirement for those personnel with significant security responsibilities as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3, and Office of Management and Budget Circular No. A-130."

Response/Action: Concur. Of the eight employees within the agency with significant security responsibilities, five attended training resulting in approximately 63% of employees with significant security responsibilities meeting this requirement. The remaining employees are scheduled to obtain the required in FY12.

Control Weakness E: Plan of Action and Milestones - IBWC had not effectively implemented a Plan of Action and Milestones (POA&M) process. The implementation of a POA&M process is important to assess the state of the OSS security posture and to aid in oversight of IT investments.

Recommendation 8: "OIG recommends the Chief Information Officer implement a Plan of Action and Milestones (POA&M) process, and review the quarterly POA&M reports and all elements of the POA&M as required by Office of Management and Budget (OMB) Memorandum M-02-Oland OMB Memorandum M-08-21A-130."

Response/Action: Concur. The draft Plan of Action and Milestones policy and procedure, which includes controls to methodically address findings and facilitate review by the CIO on a quarterly basis is currently being reviewed by management for approval by the Commissioner. The new policy and procedure ensures all required information within each PoA&M contains required information such as resource requirements, corrective action milestones required to close the PoA&M deficiency and changes to milestones. The Office of Management and Budget's (OMB) Memorandum M-02-OI and M-08-21A-130 were reviewed to ensure those requirements are included in the new policy and procedure.

Control Weakness F: Remote Access - IBWC had not developed and implemented a remote access policy and procedure to comply with NIST requirements. NIST SP 800-53 Revision 3 states that the organization documents, monitors, and controls all methods of remote access (for example, dial-up and the Internet) to the information system, including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Recommendation 9: "OIG recommends the Chief Information Officer develop a remote access policy and procedure as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3.o. A-130."

Response/Action: Concur. The IMD is currently updating the existing Access Control policy and procedure to more adequately document the remote access process. The updated documentation will address the methods by which the agency monitors and controls all means of remote access to the information system, including remote access for privileged functions.

Control Weakness G: Continuous Monitoring - IBWC had not developed a means to implement continuous monitoring of its information technology systems. OIG found that although IBWC assessed some of the controls of the operating environment, these were manual controls and IBWC had not performed automated routine security assessments of its system environment using the framework outlined in NIST SP 800-53A. In November 2009, IBWC performed the security test and evaluation to verify compliance with its security policy guidelines and to evaluate their effectiveness against anticipated threats. In addition, IBWC ensured that a comprehensive testing activity was identified to cover all appropriate security requirements, involved all necessary individuals, and ultimately provided the information needed to support the security assessment and authorization (formerly certification and accreditation) process. However, IBWC had not expanded the process to include the

periodic re-performance of vulnerability scans for its systems or automated routine performance of such scans on its enterprise network method.

Recommendation 10: “OIG recommends the Chief Information Officer develop and implement policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for all major systems and General Support Systems (GSS). The results of such security assessments should be reviewed and Plans of Action and Milestones should be developed for the improvement of the security controls of major systems and GSS as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3, and NIST SP 800-53A.130.”

Response/Action: Concur. The IMD has acquired hardware and software that will provide the necessary tools to establish an effective continuous monitoring program. These assets will help the IMD detect and measure the effectiveness of security controls applied within the GSS. All acquired items are in the process of being configured and implemented. The IMD has already installed and configured a monitor in the general area of the IMD that automatically scrolls through the status screens of several critical systems and services in order to keep them monitored in real-time. A software application called “RedLine” which works with the enterprise email system has recently been configured to email IMD staff if any of the necessary services go down or are showing signs of failure. Additional equipment include an Intrusion Detection System (IDS), Network Admissions Control (NAC) and a Network Scanner which will all provide automated methods of detecting changes within our GSS and notify the IMD of compromised PC’s or those that may show irregular activity. With the installation of new switches at HQ’s and all field offices, the IMD will gain port level visibility of all IT assets to inform our personnel of any signs of configuration changes or unauthorized activity. The IMD has also recently installed a Solar Winds Orion network performance monitor that has greatly enhanced our ability to monitor network activity. CISCO works has also been installed which sends alerts to IMD staff when certain network activity thresholds have been exceeded or show signs of potentially dangerous activity.

Control Weakness H: Contingency Planning - IBWC’s Continuity of Operations (COOP) does not comply with NIST SP 800-34.24 IBWC had not updated its contingency plan and testing policies and procedures. Specifically, the IBWC COOP for its GSS had not been updated to reflect significant changes to the environment and testing had not been performed.

Recommendation 11: “OIG recommends that the International Boundary and Water Commission finalize the Continuity of Operations site and conduct testing for operational effectiveness as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.”

Response/Action: Concur. The IMD is in the process of updating the current COOP policy and procedure as the infrastructure at the COOP site in Las Cruces, NM continues to be developed. Both the Multiprotocol Label Switching (MPLS) and Digital Signal 3 (DS3) connectivity of the COOP site has been tested and verified. A more adequate AC unit was recently installed to accommodate the additional equipment that will be installed soon. The site is currently being used as an active offsite storage location of all data backups (HQ’s & Field Offices). In addition an environmental monitoring system was installed that will immediately alert IMD personnel of any issues with temperature, moisture or power outages at that location. The VPN appliance required for remote connection to our critical data has been installed and is being configured. This will allow for critical mission functions to continue remotely in the event of a disaster. The IMD is developing a continuity plan to be reviewed

by management to determine what level of COOP the IMD will be required to maintain, taking into consideration the financial and maintenance requirements needed.

Recommendation 12: “OIG recommends that the International Boundary and Water Commission identify an offsite backup for its three field offices in Nogales, Arizona; San Diego, California; and Yuma, Arizona as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.”

Response/Action: Resolved: The IMD has acquired the needed client to allow for the full offsite backup of all field offices. All data from these field offices are now copied on a daily (differential) and weekly (full) basis to the HQ SAN and then replicated to the offsite Las Cruces backup site. The IMD had not been able to conduct offsite backups for those three field offices due to lack of a compatible backup client with our existing Commvault backup solution and the Netware OS existing on those servers.

Recommendation 13: OIG recommends that International Boundary and Water Commission ensure that its Information Management Division is involved in the oversight of information technology assets purchases and maintained by the contractor in support of operations at the waste treatment plant in San Diego, California as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3, NIST SP 800-82, and Office of Management and Budget Memorandum M-11-33.

Response/Action: Concur. The CIO is requiring modifications to the contract in place, to ensure the IMD is notified in a timely manner, of all planned technology asset purchases, in order to provide the required level of oversight of new IT purchases and existing assets maintained by the contractor. The review process will encompass review of all hardware and software. An inventory of all existing hardware located at the contractor run facility in San Diego, CA has been completed. IT Specialists from the IMD will conduct a hardware vulnerability assessment of existing equipment at the South Bay International Waste Water Treatment Plant (SBIWTP) as soon as possible. This will result in a baseline from which to work from in order to bring their equipment into compliance with SP 800-82. The IMD will create specific PoA&M’s to act as our tracking mechanism with the contractor in order to measure their progress towards resolving those issues.

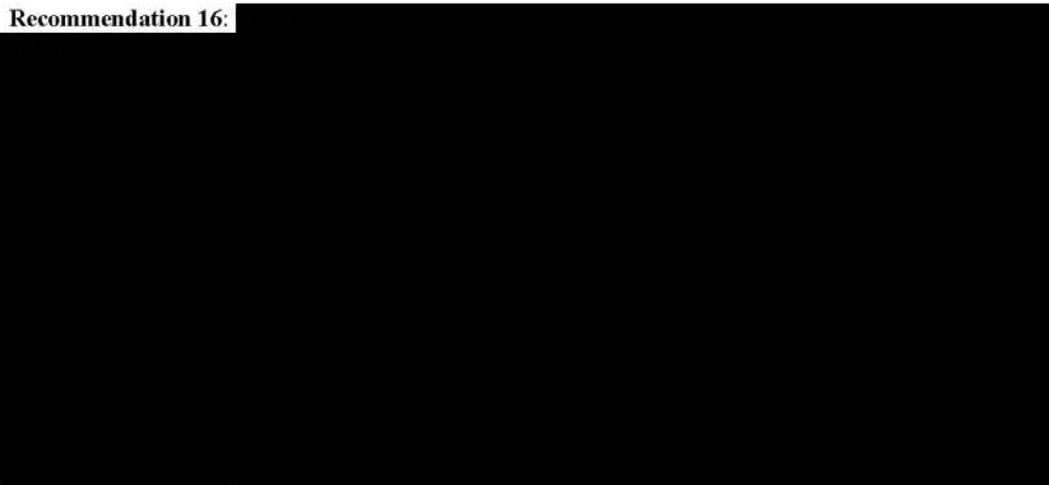
Recommendation 14: OIG recommends that International Boundary and Water Commission (IBWC) ensure that its Information Management Division reviews and approves software prior to installation on IBWC assets as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3 and Office of Management and Budget Memorandum M-11-33.

Response/Action: Concur. The CIO is requiring modifications to the contract in place, to ensure the IMD is notified in a timely manner of all planned software purchases in order to provide the required level of oversight of new IT purchases and existing software maintained by the contractor. An inventory of all non-standard software located within the contractor run systems in San Diego, CA will be conducted. IT Specialists from the IMD will conduct a software vulnerability assessment at the South Bay International Waste Water Treatment Plant (SBIWTP) as soon as possible. This will result in a baseline from which to work from in order to bring their software into compliance. The IMD will create specific PoA&M’s to act as our tracking mechanism with the contractor in order to measure their progress towards resolving those issues.

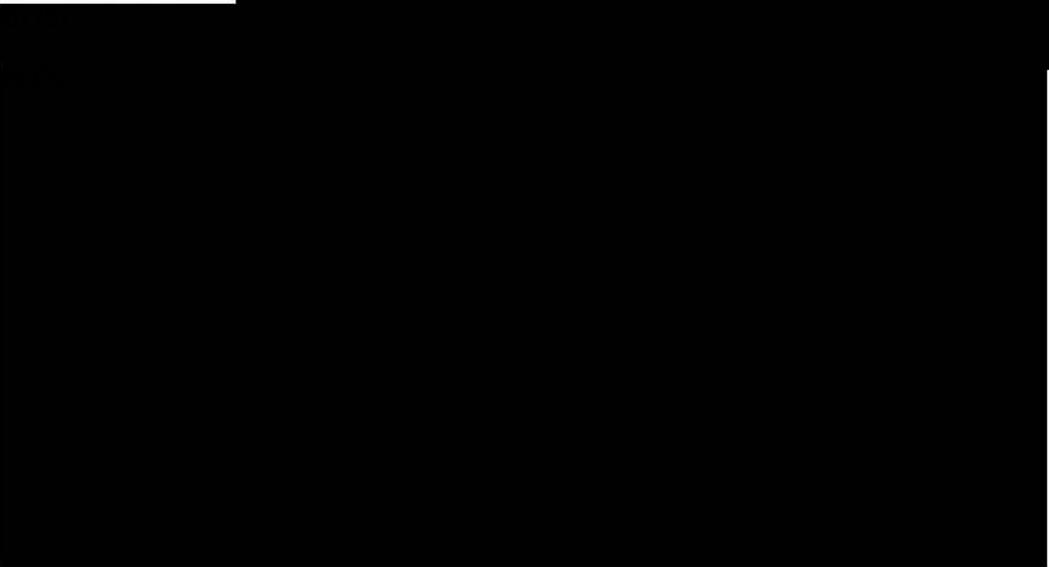
Recommendation 15: OIG recommends that the Chief Information Officer ensure that all funding for information technology (IT) security investment and IT components is tracked as required by Office of Management and Budget Memorandum M-11-33.

Response/Action: Concur. The CIO will utilize and expand upon the existing budget account structure in place, which tracks all expenses by Operating Allowance or Cost Center for all labor and non-labor costs to track all IT costs. All funding and costs for information technology (IT) security investments and IT components will be tracked consistent with Office of Management and Budget Memorandum M-11-33. In addition, the IBWC will ensure that through an effective information security program, this agency will effectively protect information and systems as well as maintain the integrity, reliability, availability, and confidentiality of our information, consistent with Office of Management and Budget Memorandum M-00-07 and M-06-19.

Recommendation 16:



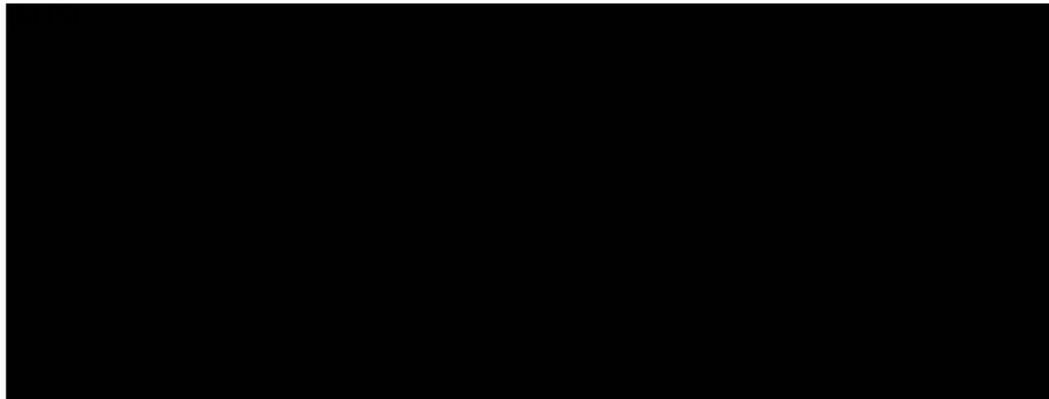
Recommendation 17:





Recommendation 19: OIG recommends the International Boundary and Water Commission (IBWC) implement a process to review, update, and approve the Information Management Division staff access list to the server room at its office in El Paso, Texas, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Response/Action: Concur. The CIO and IMD recognizes the risks associated with an unmonitored entry way into the agency's main LAN room and will take the necessary steps to implement an additional proximity card reader to limit access to only authorized IMD personnel. In addition to the existing, posted access list of authorized personnel outside of the LAN room, a process to review, update and approve the access list at least annually will be implemented.





Recommendation 21: OIG recommends the International Boundary and Water Commission (IBWC) determine the most cost effective protective measures for fire prevention and damage to file servers as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Response/Action: Concur. The CIO working with the IMD will issue specific guidance to the San Diego and Yuma Area Operations Managers, detailing actions required to remove all unnecessary items out of the server rooms to minimize or eliminate the potential of damage to equipment or injury to personnel. The new building to be occupied by IBWC personnel in Yuma, AZ will have a separate room specifically for IBWC's LAN equipment only, and will not be used for storage as is currently the case. Reviewed plans for the LAN room in that facility includes smoke and environmental detectors as well as a fire extinguisher. New building plans for the San Diego field office have not been developed yet, but as an immediate action, we have informed the staff there to remove all clutter and other flammable material from the LAN room as well as requiring them to securely bolt down the server rack to the floor as soon as possible. The Area Operations Manager will also be required to keep the LAN room secured and only allow authorized personnel.

Major Contributors to this Report

Mr. Jerry Rainwaters, Division Director Information Technology Division,
Office of Audits

Ms. Dayo Onafowokan, Auditor-in-Charge Information Technology Division,
Office of Audits

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202/647-3320
or 1-800-409-9926
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219

Please visit our Web site at oig.state.gov

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~