UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-13-39	Office of Audits	September 2013

Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

(U) PREFACE

(U) 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.

(U) 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 2013. 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.

(U) 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, personnel security, and physical and environmental protection.

(U) 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.

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

Harold W. Geisel
Acting Inspector General

(U) Acronyms

(U) BCP	Business Continuity Plan
(U) BIA	Business Impact Analysis
(U) COOP	Continuity of Operations Plan
(U) COR	contracting officer's representative
(U) DRP	Disaster Recovery Plan
(U) FISMA	Federal Information Security Management Act
(U) GIS	Geographic Information System
(U) GSS	General Support System
(U) IBWC	International Boundary and Water Commission
(U) ICS	Industrial Control System
(U) IMD	Information Management Division
(U) IT	information technology
(U) ISSM	Information System Security Manager
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) PIN	Personal Identification Number
(U) PIV	Personal Identity Verification
(U) POA&M	Plan of Action and Milestones
(U) SBIWTP	South Bay International Wastewater Treatment Plant
(U) SCADA	Supervisory Control and Data Acquisition
(U) SP	Special Publication
(U) VPN	Virtual Private Network

(U) Table of Contents

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002[1] (FISMA), the Department of State (Department), Office of Inspector General (OIG), conducted an audit of the U.S. Section, International Boundary and Water Commission (IBWC), information security program and practices. The purpose of the audit was 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). In addition, OIG reviewed IBWC's corrective actions to address weaknesses identified in OIG's FY 2012 report *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD/IT-13-15, November 2012). OIG closed four of 31 recommendations in the FY 2012 report, and IBWC had taken some action on the remaining 27 recommendations. The status of each recommendation from OIG's FY 2012 report is presented in Appendix B.

~~**(SBU)**~~ During FY 2013, OIG conducted fieldwork at IBWC's U.S. Section headquarters in El Paso, TX; South Bay International Wastewater Treatment Plant (SBIWTP) and field office in San Diego, CA, and Nogales, AZ; and the continuity of operations site in Las Cruces, NM. Overall, OIG found that IBWC had implemented an information security program and had made some progress on previously identified weaknesses. However, OIG identified security control weaknesses that, if exploited, could expose IBWC to security breaches. Specifically, the weakened security controls could adversely affect the confidentiality, integrity, and availability of IBWC information and information systems. OIG provided IBWC with 27 recommendations related to 14 security control weaknesses and identified the following six significant security deficiencies requiring immediate attention:

- ~~**(SBU)**~~ IBWC had not developed and implemented a risk management framework for its information systems. (Finding A)
- ~~**(SBU)**~~ IBWC had not implemented a continuous monitoring program for its information systems. (Finding B)
- ~~**(SBU)**~~ IBWC had not developed a comprehensive policy and procedure for implementing physical and environmental protection controls for IBWC assets. (Finding C)
- ~~**(SBU)**~~ IBWC had not implemented an effective Plan of Action and Milestones (POA&M) process. (Finding D)
- ~~**(SBU)**~~ IBWC did not have an effective capital planning process for its information systems. (Finding E)
- ~~**(SBU)**~~ IBWC had not addressed many of the critical information system components for contingency planning. (Finding F)

[1] **(U)** E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

(U) In its September 16, 2013, response (see Appendix C) to the draft report, IBWC agreed to 27 recommendations. Based on the response, OIG considers Recommendation 9 closed and the remaining 26 recommendations resolved, pending further action. IBWC's responses and OIG's replies to those responses are included after each recommendation.

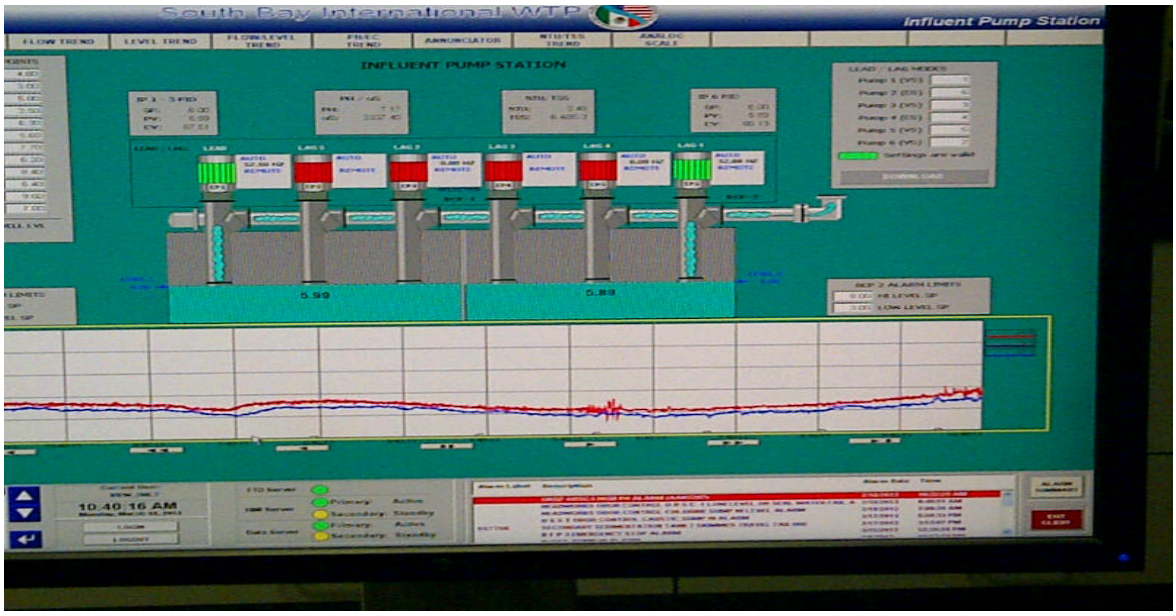
(U) Background

(U) IBWC is an international organization established in 1889 by the U.S. and Mexican Governments to apply boundary and water treaties and agreements between the United States and Mexico. IBWC consists of a U.S. Section and a Mexican Section. Each section is independent and headed by an Engineer Commissioner. The U.S. and Mexican Sections maintain their respective headquarters in the adjoining cities of El Paso and Ciudad Juárez, Chihuahua. Although IBWC is an independent international entity, the U.S. Section takes direction from the Department on matters related to foreign policy. The joint mission of the U.S. Section and the Mexican Section is as follows:

- **(U)** Distribute the waters of the boundary-rivers between the two countries.
- **(U)** Operate international flood control along the boundary-rivers.
- **(U)** Operate the international reservoirs for conservation and regulation of Rio Grande waters for the two countries.
- **(U)** Improve the quality of water of international rivers.
- **(U)** Resolve border sanitation issues.
- **(U)** Develop hydroelectric power.
- **(U)** Establish the boundary in the area bordering the Rio Grande.
- **(U)** Demarcate the land boundary.

(U) IBWC's strategic objective is to improve and sustain the quality of effluent in accordance with applicable laws and international agreements. The U.S. Section owns the contractor-operated SBIWTP, which is responsible for meeting the Clean Water Act requirements mandated by the State of California. The SBIWTP discharges the clean water into the Pacific Ocean. The U.S. Section also maintains and operates the Nogales International Wastewater Treatment Plant in accordance with the Clean Water Act discharge standards mandated by Arizona. Each wastewater treatment plant has a Supervisory Control and Data Acquisition (SCADA)[2] system. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands are controlled by remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions. A sample SCADA screen is shown in Figure 1.

[2] **(U)** A SCADA is also referred to as an Industrial Control System (ICS).



(U) Figure 1. A SCADA display at the SBIWTP. (OIG photograph)

(U) The U.S. Section is in the process of developing and implementing the necessary information technology (IT) measures to meet requirements mandated by FISMA and NIST. The agency is also in the process of acquiring and installing required software and hardware, modifying IT system configurations, and implementing policies to achieve system certification and accreditation with FISMA requirements.

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

- **(U)** 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.
- **(U)** An annual independent evaluation of the agency's information security programs and practices.
- **(U)** An assessment of compliance with FISMA requirements.

(U) FISMA assigns specific responsibilities to Federal agencies, NIST, OMB, and the Department of Homeland Security[3] 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

[3] **(U)** OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010.

inspectors general to conduct annual reviews of the agency's information security program and report the results to the Department of Homeland Security.

(U) Objective

(U) The objective of the audit was to assess the effectiveness of IBWC's information security program in FY 2013.

(U) Audit Results

(U) OIG observed that IBWC had made improvements to its security program. However, OIG identified the following control weaknesses that, if not addressed, could be detrimental to IBWC's information systems and organization. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, OIG determined that IBWC should address the 14 control weaknesses described herein.

(U) Finding A. Risk Management

~~**(SBU)**~~ In FY 2011[4] and FY 2012, OIG reported that IBWC had not developed an effective risk management program. Information Management Division's (IMD) Inventory Guide listed four information systems and one major application: two SCADA systems;[5] General Support System (GSS) and its major application, Geographic Information System (GIS);[6] and its SBIWTP Admin Network, which required identification and management of risks. NIST Special Publication (SP) 800-37, Revision 1,[7] states the following:

> **(U)** Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes.

~~**(SBU)**~~ IBWC had not developed a comprehensive governance structure and organization-wide risk management framework to include an information system perspective. NIST SP 800-37, Revision 1,[8] describes a "three-tiered risk management framework" in which tier one addresses risk from an organization perspective, tier two addresses risk from a mission and business process perspective, and tier three addresses risk from an information system

[4] **(U)** *Evaluation of the United States Section, International Boundary and Water Commission, Information Security Program* (AUD/IT-12-16, Nov. 2011).
[5] **(U)** The two SCADA systems are located in Nogales and San Diego.
[6] **(U)** GSS and GIS are located in El Paso.
[7] **(U)** NIST SP 800-37, rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, "Integrated Organization-Wide Risk Management," Feb. 2010.
[8] **(U)** Ibid.

perspective. NIST SP 800-39[9] lists "risk framing, risk assessment, risk response, and risk monitoring" as the four steps for assessing risk of information systems. A comprehensive governance structure and organization-wide risk management framework to include an information system perspective did not exist because IBWC could not identify risk management guidance to complete its draft risk management framework.

~~(SBU)~~ IBWC did not have Security Authorization Packages to include risk assessments, security plans, privacy impact assessments, and management authorizations to operate for GSS, two SCADA systems, and the SBIWTP Admin Network. In addition, IBWC's GIS did not have an application security plan. NIST SP 800-53, Revision 3,[10] requires that an organization develop, distribute, and update formal security assessments and authorization policies. Security Authorization Packages had not been completed because IBWC did not have sufficient resources to complete the necessary security documents for all IBWC information systems.

~~(SBU)~~ IBWC's GIS had an improper application classification and impact level. IBWC's IMD Inventory Guide quotes Federal Information Processing Standards 199 and states that "a major application is expected to have an impact level of moderate or high." IBWC's IMD Inventory Guide listed its GIS with a low confidentiality, integrity, and availability impact level resulting in a low impact system. GIS received a low impact level and the classification of a major application because IMD planned to include GIS in the same accreditation boundary as GSS and assumed GIS had to be classified as a major application.

~~(SBU)~~ IBWC had identified the SBIWTP Admin Network as its own information system without performing ongoing security control assessments to ensure information security requirements were in place. NIST SP 800-53, Revision 3,[11] states that organizations should "establish a continuous monitoring strategy and implement a continuous monitoring program that includes ongoing security control assessments." IBWC had not performed ongoing security controls assessments of the SBIWTP because it did not have access to the system and relied on the contractor to perform them. Without a risk management program, IBWC cannot prioritize, assess, respond to, and monitor information security risk, leaving IBWC vulnerable to outside attacks and insider threats.

> ~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission update and finalize its risk management framework to include all three tiers of managing risk, as required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, Revision 1, and the four risk management steps, as required by NIST SP 800-39.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it was in the process of finalizing a risk management framework.

[9] **(U)** NIST SP 800-39, *Managing Information System Risk*, app. E, Mar. 2011.
[10] **(U)** NIST SP 800-53, rev. 3, *Recommended Security Controls for Federal Information Systems*, "CA-1 Security Assessment and Authorization Policies and Procedures," Aug. 2009 (last updated May 2010).
[11] **(U)** NIST SP 800-53, rev. 3, "CA-7 Continuous Monitoring."

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has finalized its risk management framework to include all three tiers of managing risk.

~~(SBU)~~ Recommendation 2. OIG recommends that the International Boundary and Water Commission (IBWC) determine the ownership and classification of the South Bay International Wastewater Treatment Plant Admin Network and the Geographic Information System in accordance with Federal Information Processing Standards 199 and update the IBWC Inventory Guide.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that it is discussing ownership of the system with Veolia. IBWC further stated that it will reclassify the SBIWTP Veolia and the GIS in accordance with FIP 199 by the end of 2013.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the ownership and classification of the SBIWTP Admin Network and the GIS have been determined.

~~(SBU)~~ Recommendation 3. OIG recommends that the International Boundary and Water Commission (IBWC) develop security authorization packages for all IBWC information systems based on the determination of ownership and classification, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that the results and reclassification of the systems will be used to develop the authorization packages for all IBWC systems once the risk assessment for the GIS has been completed.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that authorization packages were developed for all IBWC information systems based on determined ownership and classification.

(U) Finding B. Continuous Monitoring

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that the IBWC did not have effective continuous monitoring management of its information systems. In FY 2013, OIG found that IBWC had not established a continuous monitoring program to include information system activity log reviews and ongoing assessments of its SCADA systems. NIST SP 800-137[12] states,

[12] **(U)** NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, "Executive Summary," Sept. 2011.

"Information security continuous monitoring is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

~~(SBU)~~ Although IBWC had procured and utilized some automated tools to perform system scans of its GSS, IBWC had not established a continuous monitoring program for all four information systems and its major application. NIST SP 800-53, Revision 3,[13] states that organizations should "establish a continuous monitoring strategy and implement a continuous monitoring program that includes ongoing security control assessments." According to the Information System Security Manager (ISSM), IBWC did not have a continuous monitoring program because it did not have all the tools in place to create a continuous monitoring strategy.

~~(SBU)~~ IBWC also did not perform ongoing vulnerability assessments of its SCADA systems. NIST SP 800-53, Revision 3,[14] states that organizations should "establish a continuous monitoring strategy and implement a continuous monitoring program that includes ongoing security control assessments." In addition, [Redacted] (b) (5) [redacted]. NIST SP 800-53, Revision 3, states that an organization "reviews and analyzes information system audit records for indications of inappropriate or unusual activity." According to IBWC officials, [Redacted] (b) (5) [redacted]

~~(SBU)~~ Without an established continuous monitoring strategy and implemented program to perform ongoing security control assessments, there is an increased risk that timely identification and mitigation of threats and vulnerabilities could remain undetected leading to potential damage or disruption of IBWC information systems.

> ~~(SBU)~~ **Recommendation 4.** OIG recommends that the Information Management Division establish a continuous monitoring strategy and implement a continuous monitoring program for all International Boundary and Water Commission information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and as outlined in NIST SP 800-137.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had implemented a continuous monitoring solution to perform vulnerability scanning and advanced risk assessment threats. IBWC further stated that it was in the process of hiring personnel and issuing a contract for continuous monitoring services.
>
> **(U) OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IMD has established a continuous monitoring strategy and implemented a continuous monitoring program for all IBWC information systems.

[13] **(U)** NIST SP 800-53, rev. 3, "CA-7 Continuous Monitoring."
[14] **(U)** Ibid.
[15] **(U)** NIST SP 800-53, rev. 3, "AU-6 Audit Monitoring, Analysis, and Reporting."

(U) Finding C. Physical and Environmental Protection

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC management had not developed and implemented effective physical and environmental protection controls for IBWC assets to include information systems. In FY 2013, OIG found that IBWC had made physical protection improvements at the SBIWTP by installing new locks to the SCADA rooms to prevent unauthorized access. Although IBWC had made improvements to physical protection, OIG observed other security deficiencies.

~~(SBU)~~ IBWC had not developed a comprehensive policy and procedure for implementing physical and environmental protection controls for IBWC assets. NIST SP 800-53, Revision 3,[16] states that an organization should develop formal, documented physical and environmental protection policies and procedures to implement physical and environmental controls.

~~(SBU)~~ SBIWTP had five gates: Gates 1, 2, and 5 provided access to the facility, and Gates 3 and 4 provided access between the United States and Mexico. [Redacted] (b) (5), [Redacted] (b) (7)(F)

[Redacted] (b) (5), [Redacted] (b) (7)(F)

[16] **(U)** NIST SP 800-53, rev. 3, "PE-1 Physical and Environmental Protection Policy and Procedures."

[Redacted] (b) (5)

[Redacted] (b) (5), [Redacted] (b) (7)(F)

~~(SBU)~~ IBWC had not maintained visitor access logs for areas where the information systems reside in El Paso, Las Cruces, San Diego, and Nogales. NIST SP 800-53, Revision 3,[18] states an organization should maintain and review "visitor access records to the facility where the information system resides." In addition, SBIWTP access cards and remote controls lacked chain of custody and could not provide accountability for personnel who accessed the facility. OIG requested documentation demonstrating chain of custody for access cards and remote controls, but no documentation was provided. In addition, OIG asked the SBIWTP Plant Superintendent to determine whether personnel accountability existed for access devices, and the Superintendent stated that IBWC [Redacted] (b) (5), [Redacted] (b) (7)(F) The Superintendent further stated that SBIWTP plans on ordering new access devices [Redacted] (b) (5), [Redacted] (b) (7)(F) NIST SP 800-53, Revision 3,[19] states that an organization should inventory physical access devices.

[18] **(U)** NIST SP 800-53, rev. 3, "PE-8 Access Records."
[19] **(U)** NIST SP 800-53, rev. 3, "PE-3 Physical Access Control."

~~(SBU)~~ OIG observed security weaknesses present in IBWC's server rooms.[20] [Redacted] (b) (5), [Redacted] (b) (7)(F)

[redacted]

~~(SBU)~~ These conditions existed because IBWC management had focused resources on maintaining mission critical operations and had not prioritized the development of a comprehensive policy and procedure to establish and implement physical and environmental protection controls for IBWC assets. Without physical and environmental protection controls, IBWC assets are not receiving the organized attention required to prevent unauthorized access or destruction, which could affect IBWC operations and result in an environmental incident.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission (IBWC) develop and implement policies and procedures for physical and environmental protection controls for IBWC assets to include information systems at headquarters and at each field office, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-82.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had developed and implemented a risk assessment policy and procedures to incorporate required physical and environmental protection controls for IBWC assets, including all information systems.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the IBWC has developed and implemented policies and procedures for physical and environmental protection controls for IBWC assets to include all of its information systems.

~~(SBU)~~ **Recommendation 6.** OIG recommends that the International Boundary and Water Commission develop and implement [Redacted] (b) (5) [redacted] as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

[20] **(U)** OIG visited all seven server rooms at the following locations: one in El Paso, one in Nogales, four in San Diego, and one in Las Cruces.
[21] **(U)** NIST SP 800-53, rev. 3, "PE-13 Fire Protection."
[22] **(U)** NIST SP 800-53, rev. 3, "PE-3 Physical Access Control."

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had established policies and procedures to control access to proximity cards and remote entrance devices.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has established policies and procedures to control access to proximity cards and remote entrance devices.

(U) Finding D. Plan of Action and Milestones

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an effective POA&M process. In FY 2013, OIG found that POA&M entries were not fully completed. In addition, POA&Ms were included in IBWC's database for vulnerabilities that did not actually exist for its information systems. Finally, [Redacted] (b) (5) [redacted] NIST SP 800-64 states, "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."

~~(SBU)~~ IBWC had incomplete POA&Ms in its database. [Redacted] (b) (5) [redacted] IBWC's POA&M Directive states, "Actual dollars or staff hours needed to correct a weakness must be identified as part of the initial corrective action plan in the 'Resources' and 'Man Hours' fields of the POA&M." The directive also states, "Each control/weakness must have at least one corresponding milestone with an anticipated completion date." POA&M entries were deficient of necessary elements because of an oversight by the ISSM.

~~(SBU)~~ The ISSM erroneously entered 174 POA&Ms in IBWC's POA&M database. NIST SP 800-53, Revision 3,[24] states that an organization should develop POA&Ms "for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system." According to the ISSM, 174 POA&Ms were recorded in the POA&M database based on information presented in a training class that he had attended; however, the 174 POA&Ms that he entered were not from supported security assessments.

~~(SBU)~~ [Redacted] (b) (5) [redacted] NIST SP 800-53, Revision 3, states that an organization should [Redacted] (b) (5) POA&Ms [Redacted] (b) (5) [redacted]

[23] **(U)** NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, Oct. 2008.
[24] **(U)** NIST SP 800-53, "CA-5 Plan of Action and Milestones."
[25] **(U)** Ibid.

[Redacted] (b) (5)

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Information Management Division update and implement its Plan of Action and Milestone Directive to include all information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had begun updating the POA&M database.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has updated its POA&M database.

~~(SBU)~~ **Recommendation 8.** OIG recommends that the Information Management Division update the Plan of Action and Milestone database [Redacted] (b) (5) as stated in the International Boundary and Water Commission Plan of Action and Milestone Directive for all information systems.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had begun updating the POA&M database.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has updated its POA&M database.

(U) Finding E. Security Capital Planning

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an effective capital planning process to include the completion of a business case/Exhibit 300/Exhibit 53. NIST SP 800-65[26] states the following:

[26] **(U)** NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, "Executive Summary," Jan. 2005.

> **(U) [**FISMA] requires agencies to integrate IT security into their capital planning and enterprise architecture processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the OMB. Therefore, the implementation of FISMA legislation effectively integrates IT security and capital planning because agencies must document resource and funding plans for IT security. Furthermore, implementation of FISMA legislation is intended to ensure that agency resources are protected and risk is effectively managed. The legislation requires that agencies incorporate IT security into the life cycle of their information systems.

~~(SBU)~~ In FY 2013, OIG found that IBWC did not have an effective capital planning process for its information systems. Specifically, IBWC did not complete a business case/Exhibit 300/Exhibit 53. NIST SP 800-53, Revision 3,[27] states that organizations should "determine, document, and allocate the resources required to protect their information systems as part of its capital planning and investment control process." NIST SP 800-53, Revision 3,[28] also states that an "organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required."

~~(SBU)~~ According to the IBWC Chief Administrative Officer, IBWC had not completed security capital planning because they were not required to complete security capital planning based on interpretation of OMB Circular A-11.[29] OMB Circular A-11 lists the legislative and judicial branches and specific executive branch agencies, along with certain Government-sponsored enterprises, as being exempt from submitting capital planning documentation. However, OMB Circular A-11 does not identify IBWC as exempt. In addition, IBWC had not completed security capital planning because the resource requirement for all POA&Ms, which helps calculate budgetary needs for its information system components, did not always exist. Finally, IBWC could not determine its information system inventory to quantify security capital funding needs. Without an effective security capital planning process, IBWC management will be unable to prioritize and remediate security weaknesses and vulnerabilities and perform equipment upgrades to support business operations.

> **(U) Recommendation 9.** OIG recommends that the International Boundary and Water Commission complete a business case/Exhibit 300/Exhibit 53 to obtain the resources required to protect its information systems, as required by National Institute of Standards and Technology Special Publication 800-65.

> **(U) Management Response:** IBWC agreed with the recommendation, stating that all of its IT assets have been inventoried and that it will continue to maintain the inventories along with associated costs.

[27] **(U)** NIST SP 800-53, rev. 3, "SA-2 Allocation of Resources."
[28] **(U)** NIST SP 800-53, rev. 3, "PM-3 Information Security Resources."
[29] **(U)** OMB Circular A-11 Part 2, *Preparation and Submission of Budget Estimates,* Aug. 2012.

(U) OIG Analysis: OIG considers the recommendation closed. Subsequent to audit fieldwork, IBWC provided documentation showing that OMB had confirmed that the requirement to complete a business case was not applicable to smaller agencies.

(U) Finding F. Contingency Planning

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an effective contingency planning program. In FY 2013, OIG found that IBWC did not have a Business Impact Analysis (BIA), Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and a Continuity of Operations Plan (COOP). A BIA identifies and prioritizes information systems and components critical to supporting the organization's mission. A BCP provides procedures for sustaining business operations while recovering from a significant disruption. A DRP provides procedures for relocating information system operations to an alternate location. A COOP provides procedures to sustain an organization's mission-essential functions at an alternate site for up to 30 days. NIST SP 800-34, Revision 1,[30] states that "contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods."

~~(SBU)~~ Although IBWC had developed the capability to virtually access a server at its alternate processing site in Las Cruces in FY 2013, it had not addressed many of the critical contingency planning components. Specifically, IBWC had not conducted a BIA, BCP, DRP, and a COOP. NIST SP 800-34, Revision 1,[31] states that an organization should "develop a contingency planning policy statement, conduct a business impact analysis, identify preventive controls, create contingency strategies, develop an information system contingency plan, ensure plan testing, training, exercises, and ensure plan maintenance." NIST SP 800-53, Revision 3,[32] defines the requirements of an organization to develop and maintain planning policies, procedures, and contingency plans. IBWC's IMD chose to focus on daily operations instead of devoting resources to developing contingency planning documents for its information systems. Without an effective contingency planning program, IBWC is at risk of not being able to access critical information and maintain business functions during an extended outage or disaster.

~~(SBU)~~ **Recommendation 10.** OIG recommends that the International Boundary and Water Commission prioritize resources to complete contingency planning documents for all information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-34, Revision 1.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had begun its BIA for the GSS, which will support its BCP and COOP documentation.

[30] **(U)** NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, "Executive Summary," May 2010.
[31] **(U)** Ibid.
[32] **(U)** NIST SP 800-53, rev. 3, "CP-1 Contingency Planning Policy and Procedures" and "CP-2 Contingency Plan."

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has completed contingency planning documents for all information systems.

(U) Finding G. Incident Response and Reporting

~~(SBU)~~ OIG first reported in FY 2012 that the IBWC did not have effective incident response and reporting. In FY 2013, OIG found that IBWC management had not approved and implemented its Incident Response Policy, correlated incidents for its GSS, and performed incident response for its SCADA systems. According to NIST SP 800-61, Revision 2,[33] "incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses, and restoring (IT) services."

~~(SBU)~~ IBWC had a draft Incident Response Policy. NIST SP 800-53, Revision 3,[34] states that an organization, "develop an incident response plan that is reviewed and approved by designated officials within the organization." IBWC's Incident Response Policy remained in draft because IBWC management had not prioritized review and approval of its policy to ensure the inclusion of all IBWC information systems.

~~(SBU)~~ Incident Response for computer security incidents did not exist for the IBWC's SCADA systems. NIST SP 800-53, Revision 3,[35] requires an organization to "implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery." Incident response had not occurred for the SCADA systems because IBWC did not have the resources and expertise.

~~(SBU)~~ IBWC did not correlate incidents identified through vulnerability scans with its incident response and reporting for its GSS. NIST SP 800-53, Revision 3,[36] requires that an organization correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. IBWC did not correlate incidents for its GSS because the Information System Security Officer had not enabled and tested the correlation capability of its vulnerability scanning software.

~~(SBU)~~ Without effective incident response and reporting, IBWC does not have the necessary capability for rapidly detecting incidents, minimizing loss and destruction, mitigating exploited weaknesses, and restoring IT services for its information systems.

~~(SBU)~~ **Recommendation 11.** OIG recommends that the International Boundary and Water Commission update, approve, and implement an incident response and reporting policy, to include the correlation of incidents for all information systems, as required by

[33] **(U)** NIST SP 800-61, rev. 2, *Computer Security Incident Handling Guide*, "Executive Summary," Aug. 2012.
[34] **(U)** NIST SP 800-53, rev. 3, "IR-8 Incident Response Plan."
[35] **(U)** NIST SP 800-53, rev. 3, "IR-4 Incident Handling."
[36] **(U)** Ibid.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-61, Revision 2.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that its Incident and Response Reporting directive is finalized and currently under review by the union.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the IBWC has established, approved, and implemented an Incident and Response Reporting Directive that includes the correlation of incidents for all information systems.

(U) Finding H. Configuration Management

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an effective configuration management process. In FY 2013, OIG found that IBWC applied untested changes to a critical information system and excluded change management for another critical information system. NIST SP 800-128[37] defines Configuration Management as "a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems."

[Redacted] (b) (5)

~~(SBU)~~ IBWC did not perform change management for its SCADA systems. NIST SP 800-82[38] states that the "change management process, when applied to the Industrial Control System (ICS), requires careful assessment by ICS experts working in conjunction with security and information technology personnel." NIST SP 800-82[39] also states, "A formal change management program should be established and procedures used to insure that all modifications to an ICS network meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans." Change management did not occur for the SCADA systems because IBWC did not have the resources and expertise to perform change management of the SCADA systems. Without implementing changes to its information systems, IBWC leaves its systems vulnerable to a denial of service and the potential introduction of security weaknesses.

[37] **(U)** NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, sec. 2.1.1, Aug. 2011.
[38] **(U)** NIST SP 800-82, sec. 3.1, "Change Management."
[39] **(U)** NIST SP 800-82, sec. 6.2.4, "ICS Specific Recommendations and Guidance."

~~(SBU)~~ **Recommendation 12.** OIG recommends that the International Boundary and Water Commission (IBWC) implement testing of all changes to its information systems, as required by the IBWC Configuration Management Directive and National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had acquired resources and hardware to implement a virtual testing environment for all changes to its information systems.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that all changes made to the IBWC information systems are tested prior to installation.

~~(SBU)~~ **Recommendation 13.** OIG recommends that the International Boundary and Water Commission update and implement its configuration management policy to include change management of Supervisory Control and Data Acquisition systems as required by National Institute of Standards and Technology Special Publication 800-82.

~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that a contract is being issued to conduct risk assessments of its SCADA systems, which includes development of configuration management policy.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has developed a configuration management policy for its SCADA systems.

(U) Finding I. Security Training

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an effective security training program. In FY 2013, OIG found that IBWC employees were not required to take initial security training before gaining access to IBWC information systems. NIST SP 800-16[40] states, "Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them."

~~(SBU)~~ OIG observed that all IBWC employees and contractors had completed their security awareness training for 2012.[41] However, employees were able to gain access to IBWC systems without taking initial security training. NIST SP 800-53, Revision 3,[42] states that the "organization provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users."

[40] **(U)** NIST 800-16, *Information Technology Security Training Requirements*, sec. 1.1, Apr. 1998.
[41] **(U)** IBWC conducts security awareness training on a calendar year basis instead of a fiscal year basis.
[42] **(U)** NIST SP 800-53, rev. 3, "AT-2 Security Awareness."

NIST SP 800-53, Revision 3,[43] also states that the "organization provides role-based security-related training before authorizing access to the system." Employees gained access to IBWC information systems without initial security training because IMD granted network access to new employees without requiring employees to complete and provide documentation that initial security awareness training had occurred. Without proper IT security training, personnel may be unaware of risks that may compromise the confidentiality, integrity, and availability of the data residing on IBWC's information systems.

> ~~(SBU)~~ **Recommendation 14.** OIG recommends that the Information Management Division ensure all new employees receive security awareness training before authorizing access to the network, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that IMD requires all new employees to complete security awareness training within 5 days of arrival and prior to obtaining network access.
>
> **(U) OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that all new employees have been required to complete security awareness training within 5 days of their arrival and prior to obtaining network access.

(U) Finding J. Remote Access Management

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an approved access control policy and effective remote access controls in place. Remote access occurs when a user (or a process acting on behalf of a user) gains access to an organizational information system by communicating through an external network. In FY 2013, OIG observed the following weaknesses for remote access management.

~~(SBU)~~ IBWC had not finalized and implemented an access control policy, a precursor to having effective remote access management. NIST SP 800-53, Revision 3,[44] states that an "organization develops, disseminates, and reviews" a formal documented access control policy to facilitate the implementation of access controls. The Commissioner had not approved IBWC's Access Control Policy, which contained a section on remote access, because the local employee union was still reviewing the policy.

~~(SBU)~~ IBWC did not require unique identification and authentication of users when logging on to IBWC's Virtual Private Network (VPN). NIST SP 800-53, Revision 3,[45] states, "The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)." [Redacted] (b) (5)

[43] **(U)** NIST SP 800-53, rev. 3, "AT-3 Security Training."
[44] **(U)** NIST SP 800-53, rev. 3, "AC-1 Access Control Policy and Procedures."
[45] **(U)** NIST SP 800-53, rev. 3, "IA-2 Identification and Authentication."

[Redacted] (b) (5)

~~(SBU)~~ None of the 55 IBWC remote access/VPN users had completed a telework agreement. The IBWC Telework Directive, dated April 24, 2012, states, "Every request for a telework arrangement must be requested using the Telework Agreement Application, IBWC Form 350 and routed through the employee's chain of command and to approving authority. All approved telework agreements are to be forwarded through the Human Resources Office for review and concurrence." IMD had not implemented its telework directive to require all personnel with remote access complete a telework agreement because it did not prioritize limited resources to produce telework agreements.

~~(SBU~~) Without taking measures to implement controls for remote access, unauthorized activities can occur without timely detection, which could affect the confidentiality, integrity, and availability of IBWC data. Inadequate remote access controls increases the risk of compromised accounts performing unauthorized activities on IBWC's information systems.

> ~~(SBU)~~ **Recommendation 15.** OIG recommends that the Information Management Division finalize and implement its access control policy, which includes remote access, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that it had finalized and implemented its access control policy.
>
> **(U) OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the IBWC access control policy has been updated and finalized to include remote access requirements.

[Redacted] (b) (5)

[46] **(U)** OMB M-06-16, *Protection of Agency Sensitive Information*, June 2006.

[redacted]

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence [Redacted] (b) (5) [redacted] identification of users.

~~(SBU)~~ Recommendation 17. OIG recommends that the International Boundary and Water Commission (IBWC) ensure all employees that require remote access capabilities for telework complete telework agreements and obtain appropriate approval, as required by IBWC's Telework Directive.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that the Telework Directive was being updated to include and document mobile workforce requirements. IBWC further stated that telework agreements were being completed by existing mobile workforce employees and should be in place by the end of 2013.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has updated its Telework Directive to include mobile workforce requirements and that IBWC's documented telework agreements are in place for existing mobile personnel by the end of 2013.

(U) Finding K. Identity and Access Management

~~(SBU)~~ OIG first reported in FY 2012 that IBWC did not have effective identity and access management for its information systems. In FY 2013, OIG found that IBWC employees did not utilize their Personal Identity Verification (PIV) cards to satisfy multifactor authentication requirements. PIV cards are identification cards that the Government issues to employees and contractors to allow authorized users physical and logical access. PIV cards are not issued until the authorizing agency has determined sound criteria for verifying an employee's identity. The full implementation of PIV cards would help IBWC meet two of three multifactor authentication requirements because an individual must "have" a physical PIV card and must "know" the card's Personal Identification Number (PIN) in order to gain physical and logical access.

~~(SBU)~~ Although OIG found that IBWC had begun to implement the use of PIV cards, not all employees were utilizing their PIV cards. [Redacted] (b) (5) [redacted] NIST SP 800-53, Revision 3, states that privileged and non-privileged accounts use multifactor authentication to access information systems. According to the ISSM, IBWC had not procured PIV card readers

[47] **(U)** NIST SP 800-53, rev. 3, "IA-2 Identification and Authentication."

for all employees, the network client software had prevented PIV process implementation, and in some cases, employees had forgotten their PINs, which prevented IBWC personnel from using their PIV cards to logically access the system. Without multifactor authentication, compromised users' identities could gain unauthorized access to sensitive information, resulting in data manipulation.

> ~~(SBU)~~ **Recommendation 18.** OIG recommends that the International Boundary and Water Commission identify and implement a multifactor authentication solution, to include a process for resetting employee Personal Identification Numbers, for logical access to information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that a two-factor authentication solution has been implemented and that the Personnel Security Policy was being updated to include procedures for resetting employee PIN for logical access to information systems.
>
> **(U) OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that a two-factor authentication solution has been implemented and that procedures have been established for resetting employees PINs for logical access to information systems.

(U) Finding L. Contractor Systems

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC had not implemented an effective oversight program for its contractor system. In FY 2013, OIG found that IBWC had not implemented a policy for oversight of its contractor-operated system. In addition, IBWC's contractor-operated system in San Diego was not compliant with contract terms and FISMA requirements. Finally, three contractors at SBIWTP had not obtained their PIV cards. OMB Memorandum M-12-20[48] states, "Agencies are fully responsible and accountable for ensuring all [FISMA] and related policy requirements are implemented and reviewed and such must be included in the terms of the contract."

~~(SBU)~~ IBWC had not fully implemented an effective oversight program that included a policy for oversight of its contractor-operated system. According to FISMA Section 3544,[49] agencies should implement policies and procedures to reduce risks for systems operated by the agency or a contractor. In addition, OIG found that the contractors lacked compliance with FISMA and the contract that IBWC produced for the operation of its SCADA system in San Diego. [Redacted] (b) (5) [redacted]. In addition, the contractors purchased equipment without the review and approval from IMD. The Amendment

[48] **(U)** OMB M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Oct. 2, 2012.
[49] **(U)** FISMA, *Title III-Information Security*, sec. 3544.

of Solicitation/Modification of Contract M027 between the IBWC and Veolia Water West Operating Services, dated April 24, 2012, states that the contractor shall achieve required compliance with FISMA for both the Supervisory Control and Data Acquisition network and the Veolia network at the SBIWTP. The contract modification also states, "prior to purchase all future IT software and hardware items for the SBIWTP shall be submitted to the IMD at IBWC for review and approval."

~~(SBU)~~ Further, three of 21 adjudicated contractors had not received their PIV cards at the SBIWTP. Homeland Security Presidential Directive 12[50] states that agencies shall require contractors to use identification in gaining physical and logical access to federally controlled facilities and information systems.

~~(SBU)~~ An effective contractor oversight program did not exist because the appointment letter for the contracting officer's representative (COR) had not addressed FISMA compliance and oversight of the SBIWTP information system. The COR believed that IMD was responsible for oversight of the IT assets. Ultimately, there was confusion on the COR responsibility to ensure FISMA compliance as the appointment letter[51] states that the COR will "[m]onitor the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan, notify the contractor of deficiencies observed during surveillance and direct appropriate action to effect correction."

~~(SBU)~~ Without proper contractor oversight, IBWC has minimal assurance that contractor personnel and operations are compliant with the contract, FISMA, and OMB requirements. In addition, there is an increased risk that data collected, processed, and maintained is exposed to unauthorized access, use, disclosure, disruption, modification, or destruction. Finally, IBWC could pay for unnecessary contractor services and products.

> ~~(SBU)~~ **Recommendation 19.** OIG recommends that the International Boundary and Water Commission develop and implement a program to include policy for information security oversight of contractors, as required by the Federal Information Security Management Act Title III, Section 3544.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that policy was being developed for information security oversight of contractors.
>
> **(U) OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that policy has been developed for information security oversight of contractors.
>
> ~~(SBU)~~ **Recommendation 20.** OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is responsible for the oversight of information technology assets purchased and maintained by the

[50] **(U)** Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, Aug. 27, 2004.
[51] **(U)** A COR was appointed by the contracting officer on Sept. 30, 2010.

contractor in support of operations at the South Bay International Wastewater Treatment Plant, as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-82.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that it had issued a contract modification to notify the contractor of IBWC's oversight requirements.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has issued a contract modification to notify the contractor of IBWC's oversight requirements.

~~(SBU)~~ Recommendation 21. OIG recommends that the International Boundary and Water Commission review and update the appointment letter of the existing contracting officer's representative at South Bay International Wastewater Treatment Plant to include responsibilities for implementing Federal Information Security Management Act (FISMA) compliance for information system assets or appoint another individual the duties for overseeing the FISMA compliance for information system assets.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that the appointment letter of the existing COR at SBIWTP was being amended to include additional responsibilities related to FISMA compliance. IBWC further stated that an appointment letter was also issued to assign the ISSM full responsibility over FISMA compliance.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the appointment letter of the existing COR at SBIWTP is amended to include additional responsibilities related to FISMA compliance and that an appointment letter has been issued to assign the ISSM full responsibility over FISMA compliance.

~~(SBU)~~ Recommendation 22. OIG recommends that the International Boundary and Water Commission (IBWC) ensure its Information Management Division reviews and approves software prior to installation on IBWC assets, as required by The Amendment of Solicitation/Modification of Contract M027.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that the contractor is required to notify IMD of all planned IT purchases and that IMD will review all purchase requests as required.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that contractors have notified IMD of all IT purchases and that IMD has reviewed and approved the use of such software prior to its purchase and installation.

(U) Finding M. Personnel Security

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC had not properly performed background screening for employees and contractors prior to granting them access to information systems and physical assets of both IBWC and the Department. IBWC had employees that were OpenNet users that worked in a variety of functions in support of IBWC operations such as budget, acquisitions, and finance. IBWC employees often need OpenNet accounts to gain access to the Global Financial Management System and Integrated Logistics Management System. Further, the onsite IMD system administrator was responsible for submitting account requests and termination information to the Department. NIST SP 800-12[52] states that "background screening helps determine whether a particular individual is suitable for a given position." IBWC made progress in addressing previously identified deficiencies regarding suitability screenings for some employees and contractors, particularly background screening for all employees designated as high-risk positions within the IMD. However, OIG identified the following deficiencies in FY 2013.

~~(SBU)~~ OIG identified 35 of 69[53] IBWC employees, designated as requiring an investigation higher than the standard National Agency Check and Inquiries. OIG found that these 35 employees had not had their investigations upgraded to meet the requirements in the IBWC Personnel Security and Suitability Directive. Specifically, within those 35 employees, OIG identified 13 of 14 Area Operation Managers or Assistant Area Operation Managers that did not have a Background Investigation performed. Area Operations Managers are located at each of the IBWC field operations and at times may be required to perform IT duties. In addition, two attorneys within the IBWC Office of General Counsel did not have the required single scope background investigation. IBWC Personnel Security and Suitability Directive requires, High Risk positions must have a Background Investigation performed. In addition, the directive states, "Investigations for Critical-Sensitive, Special-Sensitive, Moderate and High Risk positions, must be conducted pre-placement, unless a waiver is authorized." Background investigations did not occur because IBWC position descriptions did not properly incorporate the risk designation appropriate for the position, nor did the position descriptions specify the requirement to maintain an appropriate clearance level or state that the position required a background investigation. In addition, the IBWC Office of General Counsel advised the suspension of background screenings until the upgraded position descriptions are completed to reflect these requirements.

~~(SBU)~~ OIG identified 36 of 47[54] IBWC OpenNet users who were not in compliance with the memorandum that the Bureau of Diplomatic Security, Security Infrastructure, Computer Security, sent to the Bureau of Resource Management, Deputy Chief Financial Officer, Global Financial Management System, dated August 2012, regarding OpenNet extensions at IBWC. The August 2012 memorandum regarding "Annual Renewal of the OpenNet Extension at USIBWC Headquarters in El Paso, Texas," states the following:

[52] **(U)** NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, sec. 10.1.3, Oct. 1995.
[53] **(U)** OIG identified a total population of 69 IBWC employees that were designated as high-risk positions.
[54] **(U)** OIG identified a total population of 47 OpenNet users working at IBWC.

(U) All [U.S. Section] IBWC personnel that have unescorted physical and/or logical access to OpenNet must have, at a minimum, a Moderate Risk Public Trust certification (MRPT) on file with Diplomatic Security/Security Infrastructure/Office of Personnel Security and Suitability (DS/SI/PSS). USIBWC personnel security clearances must be passed to DS/SI/PSS and must be entered into the DS/SI/PSS database before granting access.

(~~SBU~~) IBWC OpenNet users did not comply with the memorandum because the Bureau of Diplomatic Security had not verified completion of required IBWC background screenings prior to granting IBWC employees' access to OpenNet. Further, the Bureau of Resource Management did not ensure compliance with the requirements of the August 2012 memorandum from Diplomatic Security/Security Infrastructure/Computer Security concerning the "Annual Renewal of the OpenNet Extension at USIBWC Headquarters in El Paso, Texas." Finally, according to IBWC management, the Bureau of Resource Management had not provided a copy of the Memorandum to IBWC to inform them of OpenNet extension compliance requirements.

(~~SBU~~) OIG found that one of 22[55] contractors at the SBIWTP had not completed the adjudication process to determine suitability, even though OIG had identified this deficiency in FY 2012. IBWC's Personnel Security and Suitability Directive states that the COR's responsibilities include "[e]nsuring compliance with all investigation and reinvestigation requirements for contractor staff." The contractor had not completed the process because the COR did not perform duties as required by the IBWC Personnel Security and Suitability Directive.

(~~SBU~~) Without full background investigations for employees, followed by adjudication and subsequent clearance, there is increased risk that individuals could gain inappropriate access to IBWC IT and physical assets. This security weakness could also affect the Department because IBWC employees would be granted access to OpenNet, a Department IT asset, without appropriate clearance levels.

(~~SBU~~) Recommendation 23. OIG recommends that the International Boundary and Water Commission update position descriptions that require background screenings, incorporate appropriate risk designations with the position, and specify the requirement to obtain and maintain the appropriate security clearance.

(~~SBU~~) Management Response: IBWC agreed with the recommendation, stating that it had updated position descriptions for all personnel who require background screenings to include appropriate risk designations and security clearance requirements.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that

[55] **(U)** OIG identified a total population of 22 contractors working at the SBIWTP.

IBWC has updated position descriptions to specify whether a background screening is required and to include appropriate risk designations.

~~(SBU)~~ Recommendation 24. OIG recommends that the International Boundary and Water Commission (IBWC) finalize suitability background screenings for both employees and contractors, to include formal adjudication and clearance, as required by IBWC's Personnel Security and Suitability Directive.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that it had finalized background screenings for all employees. IBWC further stated that formal adjudication and clearance had been accomplished for approximately half of its personnel and that the remaining personnel were awaiting results from OPM.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that IBWC has completed and adjudicated background screening for all employees and contractors.

~~(SBU)~~ Recommendation 25. OIG recommends that the International Boundary and Water Commission (IBWC), in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Computer Security, and the Bureau of Resource Management, Deputy Chief Financial Officer, Global Financial Management System, suspend IBWC employee access to OpenNet until employee background screenings are completed and adjudicated.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that its personnel security policy was being updated to incorporate the requirement to suspend IBWC employee access to OpenNet until required background screenings have been completed and adjudicated. IBWC further stated that notification of suspension will be issued to all applicable bureaus as necessary.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that policy has been developed and implemented to ensure that IBWC employee access to OpenNet is suspended until required background screening has been completed and adjudicated.

~~(SBU)~~ Recommendation 26. OIG recommends that the International Boundary and Water Commission (IBWC), Information Management Division, provide annual certification to the Department of State Bureau of Resource Management indicating that all IBWC OpenNet users fully comply with Department of State requirements concerning OpenNet access.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that it had discussed with the Department the development of a process to provide the required

annual certification indicating that all IBWC OpenNet users fully comply with the Department's OpenNet access requirements.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that a process has been developed to verify that all IBWC OpenNet users fully comply with the Department's OpenNet access requirements.

(U) Finding N. System Inventory

~~(SBU)~~ In FY 2011 and FY 2012, OIG reported that IBWC did not have an accurate information system component inventory. 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. In addition, to achieve effective property accountability, there may be information such as hardware inventory specifications and information systems/component owner that is necessary to record.

~~(SBU)~~ In FY 2013, OIG found that IBWC did not have an accurate information system component inventory that reflected its current information system assets. Although IBWC had improved its inventory tracking at the IBWC Headquarters in El Paso, OIG identified the following inventory issues at the field sites.

~~(SBU)~~ The SBIWTP information system component inventory was not complete. Specifically, OIG found instances where items on the inventory list could not be physically located and items that were physically present were not recorded on the inventory list. In addition, the documented data server inventory tag number did not match the actual data server in the San Diego field office server room. Further, the Nogales SCADA system inventory was not accurate to reflect current assets. Finally, the information system inventory listing, maintained by IMD, did not include the virtualization equipment for the continuity of operations site in Las Cruces. NIST SP 800-53, Revision 3,[56] states that organizations should "develop, document, and maintain an inventory for information system components that accurately reflects the current information system." IBWC's decentralized operations complicated the recording of IT assets because multiple personnel had a role in accounting for inventory. IMD centrally distributed IT assets to the various field offices; however, different operational elements recorded the inventory resulting in the inaccuracy of the perceived and actual inventory.

~~(SBU)~~ Without a full system inventory of IT assets, including the SCADA systems, IBWC does not have a full accounting and reporting of all IT assets resulting in the inability to mitigate security risks for its assets. In addition, IBWC may not be able to determine if assets were properly sanitized and disposed of and if inventory was stolen or inappropriately purchased.

~~(SBU)~~ **Recommendation 27.** OIG recommends that the International Boundary and Water Commission develop and implement a process for conducting and maintaining

[56] **(U)** NIST SP 800-53, rev. 3, "CM-8 Information System Component Inventory."

information system component inventory, to include all information system components concerning the Supervisory Control and Data Acquisition systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and the Federal Information Security Management Act of 2002.

~~(SBU)~~ Management Response: IBWC agreed with the recommendation, stating that inventory requirements have been incorporated into both contracts for SBIWTP systems. IBWC further stated that existing system inventory policies to conduct and maintain accountability for GSS will be implemented for all remaining systems by March 2014.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that a process has been implemented for conducting and maintaining information component inventory.

(U) List of Recommendations

~~(SBU)~~ Recommendation 1. OIG recommends that the International Boundary and Water Commission update and finalize its risk management framework to include all three tiers of managing risk, as required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, Revision 1, and the four risk management steps, as required by NIST SP 800-39.

~~(SBU)~~ Recommendation 2. OIG recommends that the International Boundary and Water Commission (IBWC) determine the ownership and classification of the South Bay International Wastewater Treatment Plant Admin Network and the Geographic Information System in accordance with Federal Information Processing Standards 199 and update the IBWC Inventory Guide.

~~(SBU)~~ Recommendation 3. OIG recommends that the International Boundary and Water Commission (IBWC) develop security authorization packages for all IBWC information systems based on the determination of ownership and classification, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 4. OIG recommends that the Information Management Division establish a continuous monitoring strategy and implement a continuous monitoring program for all International Boundary and Water Commission information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and as outlined in NIST SP 800-137.

~~(SBU)~~ Recommendation 5. OIG recommends that the International Boundary and Water Commission (IBWC) develop and implement policies and procedures for physical and environmental protection controls for IBWC assets to include information systems at headquarters and at each field office, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-82.

~~(SBU)~~ Recommendation 6. OIG recommends that the International Boundary and Water Commission develop and implement [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 7. OIG recommends that the Information Management Division update and implement its Plan of Action and Milestone Directive to include all information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 8. OIG recommends that the Information Management Division update the Plan of Action and Milestone database [Redacted] (b) (5)

[redacted] as stated in the International Boundary and Water Commission Plan of Action and Milestone Directive for all information systems. (b) (5)

~~(SBU)~~ Recommendation 9. OIG recommends that the International Boundary and Water Commission complete a business case/Exhibit 300/Exhibit 53 to obtain the resources required to protect its information systems, as required by National Institute of Standards and Technology Special Publication 800-65.

~~(SBU)~~ Recommendation 10. OIG recommends that the International Boundary and Water Commission prioritize resources to complete contingency planning documents for all information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-34, Revision 1.

~~(SBU~~) Recommendation 11. OIG recommends that the International Boundary and Water Commission update, approve, and implement an incident response and reporting policy, to include the correlation of incidents for all information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-61, Revision 2.

~~(SBU)~~ Recommendation 12. OIG recommends that the International Boundary and Water Commission (IBWC) implement testing of all changes to its information systems, as required by the IBWC Configuration Management Directive and National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 13. OIG recommends that the International Boundary and Water Commission update and implement its configuration management policy to include change management of Supervisory Control and Data Acquisition systems as required by National Institute of Standards and Technology Special Publication 800-82.

~~(SBU)~~ Recommendation 14. OIG recommends that the Information Management Division ensure all new employees receive security awareness training before authorizing access to the network, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 15. OIG recommends that the Information Management Division finalize and implement its access control policy, which includes remote access, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

[Redacted] (b) (5)

~~(SBU)~~ Recommendation 17. OIG recommends that the International Boundary and Water Commission (IBWC) ensure all employees that require remote access capabilities for telework

complete telework agreements and obtain appropriate approval, as required by IBWC's Telework Directive.

~~(SBU)~~ Recommendation 18. OIG recommends that the International Boundary and Water Commission identify and implement a multifactor authentication solution, to include a process for resetting employee Personal Identification Numbers, for logical access to information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ Recommendation 19. OIG recommends that the International Boundary and Water Commission develop and implement a program to include policy for information security oversight of contractors, as required by the Federal Information Security Management Act Title III, Section 3544.

~~(SBU)~~ Recommendation 20. OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is responsible for the oversight of information technology assets purchased and maintained by the contractor in support of operations at the South Bay International Wastewater Treatment Plant, as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-82.

~~(SBU)~~ Recommendation 21. OIG recommends that the International Boundary and Water Commission review and update the appointment letter of the existing contracting officer's representative at South Bay International Wastewater Treatment Plant to include responsibilities for implementing Federal Information Security Management Act (FISMA) compliance for information system assets or appoint another individual the duties for overseeing the FISMA compliance for information system assets.

~~(SBU)~~ Recommendation 22. OIG recommends that the International Boundary and Water Commission (IBWC) ensure its Information Management Division reviews and approves software prior to installation on IBWC assets, as required by The Amendment of Solicitation/Modification of Contract M027.

~~(SBU)~~ Recommendation 23. OIG recommends that the International Boundary and Water Commission update position descriptions that require background screenings, incorporate appropriate risk designations with the position, and specify the requirement to obtain and maintain the appropriate security clearance.

~~(SBU)~~ Recommendation 24. OIG recommends that the International Boundary and Water Commission (IBWC) finalize suitability background screenings for both employees and contractors, to include formal adjudication and clearance, as required by IBWC's Personnel Security and Suitability Directive.

~~(SBU)~~ Recommendation 25. OIG recommends that the International Boundary and Water Commission (IBWC), in coordination with the Bureau of Diplomatic Security, Security

Infrastructure, Computer Security, and the Bureau of Resource Management, Deputy Chief Financial Officer, Global Financial Management System, suspend IBWC employee access to OpenNet until employee background screenings are completed and adjudicated.

~~(SBU)~~ Recommendation 26. OIG recommends that the International Boundary and Water Commission (IBWC), Information Management Division, provide annual certification to the Department of State Bureau of Resource Management indicating that all IBWC OpenNet users fully comply with Department of State requirements concerning OpenNet access.

~~(SBU)~~ Recommendation 27. OIG recommends that the International Boundary and Water Commission develop and implement a process for conducting and maintaining information system component inventory, to include all information system components concerning the Supervisory Control and Data Acquisition systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and the Federal Information Security Management Act of 2002.

(U) Appendix A

(U) Scope and Methodology

(U) The Office of Inspector General (OIG), Office of Audits, performed this audit from February 2013 through July 2013 at the International Boundary and Water Commission (IBWC) headquarters in El Paso, TX; the continuity of operations site in Las Cruces, NM; the South Bay International Wastewater Treatment Plant and field office in San Diego, CA; and the Nogales International Wastewater Treatment Plant in Nogales, AZ.

(U) OIG interviewed IBWC senior management, employees, and contractors to evaluate managerial effectiveness and operational controls in accordance with National Institute of Standards and Technology, IBWC, and the Office of Management and Budget guidance. OIG observed daily operations, obtained evidence to support OIG conclusions and recommendations, and collected written documents to supplement observations and interviews.

(U) The Federal Information Security Management Act of 2002 (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, 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.

(U) OIG conducted this audit in accordance with generally accepted government auditing standards (GAGAS). GAGAS requires an 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 objective. OIG believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

(U) OIG discussed its preliminary findings with IBWC officials on March 14, 2013. OIG also provided IBWC with Notice of Findings and Recommendations, which were discussed in detail at an exit conference held with IBWC officials on July 25, 2013.

[*] **(U)** OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010.

(U)Work Related to Internal Controls

(U) OIG assessed the adequacy of internal controls by performing manual assessments of internal controls related to the areas audited through which OIG gained an understanding of the effectiveness of IBWC's FISMA mandated information security program. OIG identified and discussed exceptions with IBWC officials to understand the reasons behind internal control challenges. Through conversations with IBWC officials, OIG gained an understanding of the policies and procedures related to IBWC's information security program. OIG learned how IBWC oversees the development of an information security program to protect information and information systems, to report timely results regarding the security posture of information and information systems, and to implement corrective measures to address previously identified FISMA findings and recommendations. OIG's conclusions on the internal control deficiencies identified during this audit are detailed in the "Audit Results" section of this report.

(U) Use of Computer-Processed Data

(U) To assess the reliability of computer-processed data, the OIG reviewed documentation related to background screening of employees. OIG traced the background screening documentation to position descriptions to determine what individuals required additional background screening to perform their daily duties. OIG also used IBWC's inventory listing retrieved from the Integrated Logistics Management System to determine if the documented inventory matched the actual inventory at each site. OIG determined that the data were sufficiently reliable to support the conclusions and recommendations presented in this report.

(U) Appendix B

(U) Office of Inspector General
FY 2012 Federal Information Security Management Act Report
Statuses of Recommendations

(U) The FY 2012 Federal Information Security Management Act (FISMA) audit was conducted by the Department of State, Office of Inspector General (OIG), Office of Audits, and contained 31 recommendations.[*] The audit team reviewed remedial actions implemented by U.S. Section International Boundary and Water Commission (IBWC) management to respond to the findings identified in the OIG FY 2012 FISMA report. Below is the status of each recommendation:

(U) Recommendation 1. OIG recommends that the Chief Information Officer conduct an inventory to identify all information technology assets, including Supervisory Control and Data Acquisition systems for International Boundary and Water Commission.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 27 (Finding N) in the FY 2013 report.*

(U) Recommendation 2. OIG recommends that the Chief Information Officer conduct an annual inventory of information technology assets and update the full system inventory when changes are made to those information systems operated by or under the control of the International Boundary and Water Commission (IBWC) or by third-party contractors or agencies on behalf of IBWC, as required by the Federal Information Security Management Act.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 27 (Finding N) in the FY 2013 report.*

(U) Recommendation 3. OIG recommends that the Chief Information Officer develop a risk management strategy, which includes the information technology strategic plan and the enterprise architecture at the organizational level, for assessing, addressing, and monitoring information security risks, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 1 (Finding A) in the FY 2013 report.*

(U) Recommendation 4. OIG recommends that the Chief Information Officer complete the security documents and the testing of International Boundary and Water Commission information technology assets.

---

[*] **(U)** *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD/IT-13-15, Nov. 2012).

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 3 (Finding A) in the FY 2013 report.*

~~(SBU)~~ Recommendation 5. OIG recommends that the Chief Information Officer develop the security assessment and authorization packages for the Geographic Information System and Supervisory Control and Data Acquisition systems and update the security assessment and authorization package for the General Support System, as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3 and NIST SP 800-82.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 3 (Finding A) in the FY 2013 report.*

(U) Recommendation 6. OIG recommends that the Chief Information Officer improve existing procedures to ensure security assessment and authorization packages, system security plans, and security assessment reports are updated, as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-37, Revision 1 and NIST SP 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 3 (Finding A) in the FY 2013 report.*

(U) Recommendation 7. OIG recommends that the Chief Information Officer ensure that annual security assessments of a subset of a system's security controls are conducted, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 3 (Finding A) in the FY 2013 report.*

(U) Recommendation 8. OIG recommends the Chief Information Officer develop and implement configuration management and testing procedures including, but not limited to, patch management and periodic assessments of compliance with the implemented procedures, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-40, Version 2.0.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendations 12 and 13 (Finding H) in the FY 2013 report.*

(U) Recommendation 9. OIG recommends that the Chief Information Officer develop and implement procedures for the oversight of all systems and hardware including, but not limited to, patch management and periodic assessments of compliance with implemented procedures 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.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 13 (Finding H) in the FY 2013 report.*

(U) Recommendation 10. OIG recommends the Chief Information Officer incorporate the updated incident report template into the incident response and reporting procedures and periodically assess compliance with the procedures, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 11 (Finding G) in the FY 2013 report.*

(U) Recommendation 11. OIG recommends that the Chief Information Officer ensure the security awareness training policy requiring all International Boundary and Water Commission personnel to attend initial security awareness training is finalized and then ensure that the personnel take the training before they are provided access to information technology systems, 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.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 14 (Finding I) in the FY 2013 report.*

(U) Recommendation 12. OIG recommends that the Chief Information Officer ensure all International Boundary and Water Commission personnel attend security awareness refresher training and suspend access to information technology systems and assets when personnel fail to successfully complete the 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.

(U) *Status: Closed March 2013.* IBWC provided evidence of security awareness training completion for IBWC's employees and contractors for 2012.

(U) Recommendation 13. OIG recommends that the Chief Information Officer ensure the specialized security training requirement for International Boundary and Water Commission personnel with significant security responsibilities is completed so that the personnel are able to maintain their professional proficiency, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2013.* IBWC provided evidence of whom they have identified as having additional security responsibilities and provided evidence of their training completion for 2012.

(U) Recommendation 14. OIG recommends the Chief Information Officer fully implement a Plan of Action and Milestones process to include vulnerabilities identified from all sources and update milestone dates, as required by Office of Management and Budget Memorandum M-08-21 and NIST Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 7 (Finding D) in the FY 2013 report.*

(U) Recommendation 15. OIG recommends that the Chief Information Officer finalize and implement International Boundary and Water Commission remote access policy and procedure, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 15 (Finding J) in the FY 2013 report.*

~~(SBU)~~ Recommendation 16. OIG recommends that the Chief Information Officer implement remote access controls that is enforced with two-factor authentication and encryption of data on mobile devices, as required by the Office of Management and Budget Memorandum M-06-16.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 16 (Finding J) in the FY 2013 report.*

~~(SBU)~~ Recommendation 17. OIG recommends that the Chief Information Officer develop and implement a wireless policy and procedures, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 15 (Finding J) in the FY 2013 report.*

(U) Recommendation 18. OIG recommends that the Chief Information Officer update and implement identification and authentication management procedures to include the e-authentication procedures, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed June 2013*. IBWC provided evidence that the IBWC Access Control policy had been finalized and that it included details on the use of Personal Identity Verification cards.

(U) Recommendation 19. OIG recommends that the Chief Information Officer perform a risk assessment identifying the risks to system security, as required by the Office of Management and Budget Memorandum M-04-04.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 3 (Finding A) in the FY 2013 report.*

~~(SBU)~~ Recommendation 20. OIG recommends that the Chief Information Officer develop and implement policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for the General Support System, the Geographical Information System, and the Supervisory Control and Data Acquisition systems. 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, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 4 (Finding B) in the FY 2013 report.*

~~(SBU)~~ Recommendation 21. OIG recommends that the International Boundary and Water Commission develop and implement contingency planning procedures and conduct testing for operational effectiveness of all major systems, as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 10 (Finding F) in the FY 2013 report.*

~~(SBU)~~ Recommendation 22. OIG recommends that the International Boundary and Water Commission finalize the continuity of operations site and conduct testing for operational effectiveness of all major systems, as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 10 (Finding F) in the FY 2013 report.*

(U) Recommendation 23. OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is responsible for the oversight of information technology assets purchased and maintained by the contractor in support of operations at the wastewater treatment plant in San Diego, CA, as required by National Institute of Standards and Technology Special Publications (SP) 800-53, Revision 3, and SP 800-82.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 20 (Finding L) in the FY 2013 report.*

(U) Recommendation 24. 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.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 22 (Finding L) in the FY 2013 report.*

(U) Recommendation 25. OIG recommends that the Chief Information Officer ensure that all information technology assets are accounted for, reported and tracked, and used in the calculation and reporting of Exhibit 300/Exhibit 53's to the Office of Management and Budget. Additionally, OIG recommends that International Boundary and Water Commission incorporate funding requirements in the information technology strategic plan, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 9 (Finding E) in the FY 2013 report.*

(U) Recommendation 26. OIG recommends that International Boundary and Water Commission finalize its contractors' suitability clearances, including formal clearance adjudication, and issue badges, as required by Homeland Security Presidential Directive 12.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 24 (Finding M) in the FY 2013 report.*

(U) Recommendation 27. OIG recommends that International Boundary and Water Commission ensure that the adjudication process is completed for the information technology employees undergoing background investigations.

(U) *Status: Closed March 2013.* IBWC has performed background investigations on all employees within the Information Management Division to be in accordance with their high-risk position designation as stated in the IBWC Personnel Security and Suitability Directive.

(U) Recommendation 28. OIG recommends that the International Boundary and Water Commission develop and implement chain-of-custody procedures to control access to the proximity access cards and remote gate devices along the international border.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 6 (Finding C) in the FY 2013 report.*

(U) Recommendation 29. OIG recommends that the International Boundary and Water Commission develop and implement physical access controls to restrict access to the Supervisory Control and Data Acquisition control centers, Programmable Logic Controller, and file servers, as required by National Institute of Standards and Technology Special Publication 800-82.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 5 (Finding C) in the FY 2013 report.*

(U) Recommendation 30. OIG recommends that the International Boundary and Water Commission restrict access to file servers at its San Diego, CA, wastewater treatment plant, the field offices in Fort Hancock, TX, and its headquarters in El Paso, TX, and ensure the servers are attached to the floor to prevent damage to equipment or harm to employees, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 5 (Finding C) in the FY 2013 report.*

(U) Recommendation 31. OIG recommends that the International Boundary and Water Commission determine the most cost-effective protective measures to prevent fire and damage to file servers, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed from the FY 2012 FISMA report. This recommendation has been reissued as Recommendation 5 (Finding C) in the FY 2013 report.*

(U) Appendix C

OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

September 16, 2013

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

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

Dear Mr. Geisel:

We appreciate the opportunity to provide responses to the FY 2013 audit findings and recommendations (attached) represented in your draft report of September 3, 2013. We are committed to giving these our highest priority and we will continue to keep your office posted on our continued progress towards full implementation of all recommendations.

Please advise if you have any questions or if we may be of any assistance.

Sincerely,

Edward Drusina, P.E.
Commissioner

Attached: as stated

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

Office of Audits

International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program

AUD-IT-13-XX
August 2013

1

U) Finding A. Risk Management

~~(SBU)~~ **Recommendation 1. Agree:** A risk management framework is being finalized.

(SBU) Recommendation 2. Agree. Discussions with Veolia are ongoing where ownership of the Systems will be made clear. Reclassifications of the SBIWTP Veolia and GIS Systems in accordance with FIPS 199 will be completed by the end of the calendar year.

~~(SBU)~~ **Recommendation 3. Agree.** The IBWC has issued a contract for a risk assessments of the South Bay International Wastewater Treatment Plant (SBIWTP) SCADA, Admin and Nogales International Wastewater Treatment Plant SCADA Systems. The Geographic Information System risk assessment is being finalized. The results of the risk assessments and reclassification of Systems will be used to develop authorization packages for all IBWC Systems.

(U) Finding B. Continuous Monitoring

~~(SBU)~~ **Recommendation 4. Agree.** A continuous monitoring solution is now in place to perform vulnerability scanning and advanced risk and threat assessments; actions are under way to hire personnel and issue a contract for continuous monitoring services. The IBWC will be accepting an invitation to participate in the Department of Homeland Security's (DHS) Continuous Diagnostic and Mitigation (CDM) Program, which will provide authorized vendors to perform these functions for federal agencies.

(U) Finding C. Physical and Environmental Protection

~~(SBU)~~ **Recommendation 5. Agree**. The IBWC has developed and implemented a risk assessment policy and procedures, which incorporates the requirement for physical and environmental protections controls for IBWC assets. In addition, the Master Planning Division (MPD) of the IBWC will be conducting assessments of all facilities to include all information system (IT/server rooms) locations and ensure that physical and environmental protection controls exist or implemented in accordance with NIST SP 800-53, Rev 3 and NIST SP800-82. Designs for ongoing new admin building facilities already include all physical and environmental requirements

[Redacted] (b) (5)

2

(U) Finding D. Plan of Action and Milestones

~~(SBU)~~ **Recommendation 7. Agree.** The Information Management Division has updated its PoAMs database, which now exclude the 174 entries that were not derived from a supported security assessment. Other updates are being made to the PoAMs database to include all elements identified during the OIG FISMA audit, and in accordance with NIST SP 800-53, Rev 3.

~~(SBU)~~ **Recommendation 8. Agree.** The Information Management Division approaching completion of its update to the Plan of Action and Milestone database, [Redacted] (b) (5)

(U) Finding E. Security Capital Planning

(U) Recommendation 9. Agree. The IBWC has inventoried all its IT assets and will continue to document all assets and maintain the inventory updated, along with associated costs. The IBWC will also continue to represent its needs in future budget requests to ensure required resources are available to protect its information systems. Development of Exhibit 300 and 53 is required of all CFO agencies consistent with OMB Circular A-11 guidance, which is not the designation of the IBWC. OMB representatives have confirmed that the requirement is not applicable to small agencies.

(U) Finding F. Contingency Planning

~~(SBU)~~ **Recommendation 10. Agree.** The IBWC has begun its Business Impact Assessment for the GSS which will feed its Business Continuity Plan and Continuity of Operations documentation as required. Contingency planning documentation for all other systems are being planned and developed as required by SP-800-53 and NIST SP 800-34, Rev 1

(U) Finding G. Incident Response and Reporting

~~(SBU)~~ **Recommendation 11. Agree.** The IBWC has finalized its Incident and Response Reporting directive, which is currently under review by the union.

(U) Finding H. Configuration Management

~~(SBU)~~ **Recommendation 12. Agree.** The IBWC has acquired the resources and hardware to implement a virtual testing environment to test all changes to its information systems as

required by the existing directive and NIST SP 800-53, Rev 3.
~~(SBU)~~ **Recommendation 13. Agree.** The IBWC is issuing a contract to conduct risk assessments of the two SCADA systems, which includes development of configuration management policy.

(U) Finding I. Security Training

~~(SBU)~~ **Recommendation 14. Agree.** The IMD has effectively assured that all new employees complete the required security awareness training within 5 days of their arrival in order to obtain authorization to access the network. The established process is being followed in accordance with IBWC policy SD.I.6061-M-111 Security Awareness and Training.

(U) Finding J. Remote Access Management

~~(SBU)~~ **Recommendation 15. Agree.** The IBWC has finalized and implemented its access control policy.

[Redacted] (b) (5)

(SBU) Recommendation 17. Agree. The Telework Directive is being updated to correctly include and document mobile workforce requirements. Telework agreements for existing mobile workforce employees are being completed and will be in place by the end of the calendar year.

(U) Finding K. Identity and Access Management

~~(SBU)~~ **Recommendation 18. Agree.** The IBWC has implemented a two-factor authentication solution, to include a process for resetting employee Personal Identification Numbers, for logical access to information systems. The Personnel Security policy is being updated to incorporate this process.

(U) Finding L. Contractor Systems

~~(SBU)~~ **Recommendation 19. Agree.** Policy is being developed for information security oversight of contractors, as required by the Federal Information Security Management Act Title III, Section 3544.

~~(SBU)~~ **Recommendation 20. Agree.** The IBWC has issued a modification to the South Bay

International Wastewater Treatment Plant contractor, notifying the contractor of IBWC's management oversight requirements of information technology assets purchased and maintained by the contractor in support of operations. A copy of the modification was previously provided.

~~(SBU)~~ **Recommendation 21. Agree.** The appointment letter of the existing contracting officer's representative at South Bay International Wastewater Treatment Plant is being amended to include responsibilities. An appointment letter has also been issued to the ISSM designating him full responsibility over FISMA compliance oversight.

~~(SBU)~~ **Recommendation 22. Agree.** The contractor is required to notify the Information Management Division of all planned purchases of IT hardware and software. The IMD will review all requests as required by The Amendment of Solicitation/Modification of Contract M027.

(U) Finding M. Personnel Security

~~(SBU)~~ **Recommendation 23. Agree.** The IBWC has updated the position descriptions of all personnel that require background screenings, which incorporate appropriate risk designations with the position, and specify the requirement to obtain and maintain the appropriate security clearance. Copies of the amendments were provided to the OIG during a previous update.

~~(SBU)~~ **Recommendation 24. Agree.** The IBWC has finalized requests for suitability background screenings for 100% of both employees and contractors, as required by its Personnel Security and Suitability Directive. Formal adjudication and clearance has been accomplished for approximately half with the second half pending receipt of results from OPM.

~~(SBU)~~ **Recommendation 25. Agree.** The IBWC is incorporating into its personnel security policy a process that requires the IBWC to suspend IBWC employee access to OpenNet until the required background are obtained. Notification will be issued to the Bureau of Diplomatic Security, Security Infrastructure, Computer Security, and the Bureau of Resource Management, Deputy Chief Financial Officer, Global Financial Management System to suspend accounts as necessary.

~~(SBU)~~ **Recommendation 26. Agree.** The IBWC is in discussions with the Department of State Bureau of Resource Management and will be developing a process to provide the required annual certification indicating that all IBWC OpenNet users fully comply with Department of State requirements concerning OpenNet access.

(U) Finding N. System Inventory

~~(SBU)~~ **Recommendation 27. Agree.** The IBWC has incorporating the necessary inventory requirements into the contract for both SBIWTP systems. In addition, the existing system inventory policies for conducting and maintaining system component accountability for the GSS will be implemented for all remaining systems by March 2014.

(U) Major Contributors to This Report

Jerry Rainwaters, Director
Division of Information Technology
Office of Audits

Jamie Horvath, Manager
Division of Information Technology
Office of Audits

Kenneth Bensman, Senior Auditor
Division of Information Technology
Office of Audits

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT OF FEDERAL PROGRAMS HURTS EVERYONE.

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320
800-409-9926
oighotline@state.gov
oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219