UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-13-15	Office of Audits	November 2012

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

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

(U) Acronyms

(U) CM	configuration management
(U) FISMA	Federal Information Security Management Act
(U) GIS	Geographic Information System
(U) GSS	General Support System
(U) IBWC	United States Section, International Boundary and Water Commission
(U) IMD	Information Management Division
(U) IT	information technology
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) POA&M	Plan of Action and Milestones
(U) SCADA	Supervisory Control and Data Acquisition
(U) SP	Special Publication

(U) Table of Contents

(U) Section **(U)** Page

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002,[1] (FISMA) the Department of State, Office of Inspector General (OIG), conducted an audit of the U.S. Section, International Boundary and Water Commission (IBWC), information security program and practices to determine compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). In addition, OIG reviewed remedial actions taken by IBWC to address control weaknesses identified in OIG's FY 2011 report *Evaluation of the United States Section, International Boundary and Water Commission, Information Security Program* (AUD/IT-12-16, November 2011). IBWC took corrective actions on four of 21 recommendations in the FY 2011 report, and OIG considers the recommendations closed. The statuses of the remaining recommendations from OIG's FY 2011 report are presented in Appendix B.

(U) OIG reviewed systems at IBWC's U.S. Section headquarters in El Paso, TX; field offices in San Diego, CA, Yuma, AZ, and Fort Hancock, TX; and continuity of operations site at 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. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, IBWC should address the following 14 security control weaknesses:

A. (U) System Inventory

(U) As reported by OIG for FY 2011,[2] IBWC's inventory management process to update and manage its information technology (IT) assets should be improved. IBWC's inventory of systems consists of four information systems: the General Support System (GSS), Geographic Information System (GIS), the Nogales Supervisory Control and Data Acquisition (SCADA) system in Arizona, and the San Diego SCADA system in California. IBWC performed an inventory of its hardware and systems during FY 2012; however, because an IBWC official was unaware of a requirement to update system inventory when hardware changes occurred, IBWC could not fully account for all IT assets. IBWC had not fully implemented the IBWC Information Technology System Inventory Guide procedures, which require a complete inventory annually. Without a full system inventory management process for all IT assets, IBWC may not have an accurate accounting of all related system interfaces or underlying support systems and may not be able to properly identify and mitigate security risks.

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

[2] **(U)** *Evaluation of the United States Section, International Boundary and Water Commission, Information Security Program* (AUD/IT-12-16, Nov. 2011).

B. (U) Risk Management Program

(U) As reported by OIG for FY 2011, IBWC had not implemented a risk management framework or information security policies and procedures that describe the roles and responsibilities of key participants at the organization and system levels. IBWC had neither developed the enterprise architecture nor integrated the IT Strategic Plan into the budget process as part of the risk management program. Since the enterprise architecture and the strategic plan have not been considered in the risk management program, IBWC may not be requesting funding levels appropriate to the risk exposure. Without the implementation of the risk management strategy at the organizational level, the communication of operations at the system level and funding allocation could be negatively affected because plans have not been developed to deal with risk exposure. As such, management is not fully aware of the security vulnerabilities that exist.

~~(SBU)~~ At the information system level, IBWC had not completed the security assessment authorization package for any of the systems. (b) (5) [redacted] IBWC officials stated that IBWC was unaware of the requirement to complete the security assessments and authorization package for GIS. The requirement by NIST for updating GSS and the SCADA systems had not been completed because of the lack of available resources. Without a security assessment and authorization in place, IBWC's risk management framework is weakened and IBWC does not have the ability to assess, address, and monitor information security risk.

C. (U) Configuration Management

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not implemented effective configuration management (CM) standards and procedures for its IT environment. Although, IBWC had CM standards and procedures in place, IBWC had not implemented a change control process that involved the systematic proposal, justification, implementation, test and evaluation, review, and disposition of changes to the system, including upgrades and modifications. Without implemented procedures that govern the performance of the CM processes, IBWC will not be able to effectively manage the IT security program, which could lead to the introduction of security weaknesses and inconsistent performance.

[3] **(U)** NIST SP 800-37, rev.1, "Guide for Applying the Risk Management Framework to Federal Information Systems," Feb. 2010.

D. (U) Incident Response and Reporting

(U) IBWC's incident response and reporting did not fully comply with NIST SP 800-53, Revision 3.[4] Specifically, IBWC had not updated its incident response policy and procedures to reflect changes made to its reporting documentation. An IBWC official stated that the incident report template had been updated but had not been incorporated into the incident response and reporting procedures. Lack of an updated procedure may prevent IBWC from reporting security incidents to appropriate authorities.

E. (U) Security Training

(U) As reported by OIG for FY 2011, IBWC had not trained all employees and contractors as required by its security awareness training program. At the time of OIG's fieldwork conducted in April 2012, IBWC employees had not completed their general security awareness training, and not all employees with significant security responsibilities had completed their specialized training. However, 5 months remained in the fiscal year during which IBWC could have satisfactorily fulfilled the training requirements. Although IBWC had acquired a security awareness training product in April 2012, an IBWC official stated that the product had not been implemented. Without the completion of initial and annual security awareness training, personnel may be unaware of new risks that may compromise the confidentiality, integrity, and availability of data. Employees with significant security responsibilities who are not properly trained create a risk for IBWC because they may present vulnerabilities or may cause security breaches.

F. (U) Plan of Action and Milestones

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not fully implemented an effective Plan of Action & Milestone (POA&M) process. Although IBWC had made improvements in its POA&M process by including details of the estimated resource requirements and corrective action plans to close the POA&M deficiencies, as required in the OMB template, OIG determined that POA&Ms (1) did not include all vulnerabilities, (2) did not demonstrate that milestones were being effectively addressed to update the status of changes, and, (3) were not always reviewed by the Chief Information Officer. IBWC had not determined the security weaknesses for GIS and the SCADA systems because IBWC had not completed the necessary security documents identifying the security controls in place and those that required improvement. System security plans and an independent assessment (Security Test and Evaluation report) would identify the controls that are in place and those that are either missing or deficient (are not up to the standard required by Federal Information Processing Standards [FIPS] Publication 199[5] levels of potential impact on organizations associated with the system). The absence of

[4] **(U)** NIST SP 800-53, rev. 3, "Recommended Security Controls for Federal Information Systems and Organizations," IR-1 through IR-8, Aug. 2009 (last updated May 2010).

[5] **(U)** FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," Feb. 2004.

these security documents indicated to OIG that IBWC had not conducted the necessary testing of GIS and the SCADA systems; therefore, IBWC was unable to identify the weaknesses requiring remediation. Additionally, IBWC was conducting periodic security scans of GSS, but the weaknesses that were identified in those scans were also not being recorded in the POA&Ms. Without periodic updates and reviews of POA&M activities and/or completion of necessary security tests and evaluations, IBWC management may be unaware of the statuses of security vulnerabilities or of associated corrective actions.

G. (U) Remote Access

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not finalized and implemented its remote access policy and procedures to comply with the requirements in NIST SP 800-53, Revision 3.[6] (b) (5) [redacted] An IBWC official stated that the access control policy and procedures document contained procedures for remote access, but OIG determined that the procedures still required review and formal approval by IBWC management. Further, an IBWC official stated that controls had not been fully implemented for remote access because of a lack of resources.

~~(SBU)~~ In addition, IBWC did not have a wireless policy and procedure in place for establishing usage restrictions and implementation guidance for wireless access, monitoring for unauthorized wireless access to the information system, authorizing wireless access to the information system prior to connection, or enforcing requirements for wireless connections to the information system. Without proper controls in place, unauthorized activities can occur without timely detection, which could adversely impact confidentiality, integrity, and availability of the data.

H. (U) Identity and Access Management

~~(SBU)~~ IBWC had not implemented its identity and access management process. Although IBWC had an Identification and Authentication Policy and Procedure, the policy had not been reviewed and updated to reflect changes since 2009. OIG determined that the personal identity verification cards were configured to the network prior to any testing or assessment performed, as required by OMB Memorandum M-04-04.[7] However, a risk assessment identifying the risk to the system security had not been performed. An IBWC official stated that no formal risk assessment had been performed prior to the implementation of the personal identity verification card because IBWC was not aware that a requirement needed to be completed. Inadequate identity and access management controls increase the risk that accounts may be accessed and used by individuals to perform unauthorized activities.

[6] **(U)** NIST SP 800-53, rev. 3, AC-17 "Remote Access," Aug. 2009 (last updated May 2010).

[7] **(U)** OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," Dec. 16, 2003.

I. (U) Continuous Monitoring

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not fully implemented a continuous monitoring program of its IT systems. During 2012, IBWC had assessed and installed a vulnerability management tool to perform automated routine security assessments of its system environment. However, IBWC manually initiated the vulnerability scans on its enterprise network because of configuration issues between the vulnerability management tool and the network. In addition, IBWC had not developed a formal process to include performing periodic vulnerability scans on its enterprise network, reviewing firewall logs, monitoring unauthorized devices, and, tracking centrally vulnerability results. An IBWC official stated that because of limited resources there were no documented policies and procedures detailing the strategy and plans for conducting continuous monitoring activities that included scanning routinely for vulnerabilities, monitoring logs, and notifying appropriate officials of unauthorized devices. Without periodic reviews or the performance of risk-based security assessments, new threats and vulnerabilities may not be identified and mitigated in a timely manner.

J. (U) Contingency Planning

~~(SBU)~~ As reported by OIG for FY 2011, significant improvements were needed to strengthen the IBWC contingency planning process. Although IBWC had documented a contingency plan for GSS and had configured an automated backup process for the headquarters and field offices, b) (5) [redacted]

K. (U) Oversight of Contractor System

(U) As reported by OIG for FY 2011, IBWC had not implemented an effective oversight program of its contractor system. IBWC's San Diego field office did not have documented policies and procedures for IBWC's oversight of systems operated by contractors and did not include the SCADA operations within IBWC's IT boundaries. An IBWC official stated that IBWC was aware of the deficiencies and was working to address the issues. OIG determined that IBWC officials did not have adequate control over the IT functions at the San Diego wastewater treatment plant or over the IT assets purchased and maintained by the contractor in support of operations. Without proper oversight, there is an increased risk that data collected, processed, and maintained could be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

L. (U) Security Capital Planning

(U) As reported by OIG for FY 2011, information security was not integrated into IBWC's Capital Planning and Investment Control process. IBWC did not provide OMB with a detailed explanation for the major investment related to its IT capital investment. An IBWC official stated that because of the small size of the organization, IBWC officials believed IBWC budget requirements did not meet the level established for reporting to OMB. Lack of planning increases the risk that requests for funding investments will not receive proper consideration.

M. (U) Personnel Security

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had developed its personnel security program but needed to continue making improvements to its implementation of the program because of weaknesses identified by OIG in FY 2011. OIG determined that overall progress had been made toward the implementation of an effective personnel security program. An IBWC official stated that the review process was still ongoing because of limited resources. However, without fully investigating each employee's background, followed by the adjudication process and subsequent clearance, the potential existed for IBWC to employ personnel who were not adequately qualified for selected positions. In addition, employees may be granted inappropriate administrator permissions to access IBWC information technology and physical assets.

N. (U) Physical and Environmental Protection

~~(SBU)~~ As reported by OIG for FY 2011, significant improvements were necessary for IBWC to strengthen its physical and environmental protection controls of organizational assets. Although IBWC had implemented a manual log process for IBWC San Diego contractors to account for the entry and exit of Mexican trucks through the international boundary gate (b) (5) [redacted]

~~(SBU)~~ IBWC did not enforce physical access authorizations to the information system independent of the physical access controls for the facility. Although physical access controls were in place at the plant, (b) (5) [redacted]

(U) Based on fieldwork completed in 2012, OIG made 31 recommendations and identified six significant security deficiencies requiring immediate attention as follows:

- **~~(SBU)~~** IBWC had not implemented a risk management framework or information security policies and procedures that describe the roles and responsibilities of key participants at the organization and system levels. (Finding B)
- **~~(SBU)~~** IBWC had not implemented effective CM standards and procedures for its IT environment. (Finding C)
- **(U)** IBWC had not fully implemented an effective POA&M process. (Finding F)
- **(U)** IBWC had not fully implemented a continuous monitoring program of its IT systems. (Finding I)
- **(U)** IBWC's San Diego field office had not documented policies and procedures for oversight of its systems operated by contractors and did not include the SCADA systems operations within its IT boundaries. (Finding K)
- **~~(SBU)~~** IBWC had implemented a manual log process for IBWC San Diego contractors to monitor and track Mexican trucks moving through the international boundary gate, (b) (5) [redacted]

(U) In October 2012, OIG provided a draft of this report to IBWC. Based on IBWC's October 30, 2012, response to the report's 31 recommendations, OIG considers all of the recommendations resolved, pending further action.

(U) IBWC's responses to each recommendation and OIG's replies to these responses are presented after each recommendation. (IBWC's response is in Appendix C.)

(U) Background

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

(U) The entity was created as the International Boundary Commission by the Convention of 1889[8] and given its current name under the Treaty of 1944.[9] IBWC consists of the U. S. Section and the Mexican Section, which have their headquarters in the adjoining cities of El Paso, TX, and Ciudad Juárez, Chihuahua, respectively. Although IBWC is an independent international entity, the U. S. Section takes direction from the Department of State on matters related to foreign policy. The Mexican Section is a unit in the Mexican Ministry of Foreign Affairs.

[8] **(U)** The Convention of March 1, 1889, was held to address the difficulties caused by natural changes that take place in the beds of the Rio Grande and Colorado Rivers. U.S.-Mex., Mar. 1, 1889, 26 Stat. 1512 (extended indefinitely by Article II of the treaty signed Feb. 3, 1944, 59 Stat. 1219).

[9] **(U)** Utilization of Waters of the Colorado and Tijuana Rivers and of the Rio Grande, U.S.-Mexico, art. II, Feb. 3, 1944, 59 Stat. 1219.

(U) Through a series of treaties and agreements, IBWC is charged with the application, regulation, and exercise of the provisions of such treaties and agreements for the solution of water and boundary issues along the 1,954-mile border between the two countries. The U. S. Section of IBWC operates under the provisions of 22 U.S.C. 277.[10] The joint mission of the U. S. Section and the Mexican Sections 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 limitrophe to (bordering) the Rio Grande.
- **(U)** Demarcate the land boundary.

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

(U) The Act[11] assigns specific responsibilities to Federal agencies, NIST, OMB, and the Department of Homeland Security[12] 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

[10] **(U)** 22 U.S.C. § 277, "International Boundary Commission, United States and Mexico; study of boundary waters."
[11] **(U)** E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).
[12] **(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.

effectiveness of information system controls, FISMA requires agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to the Department of Homeland Security.

(U) Objective

(U) The objective of this audit was to determine the effectiveness of IBWC information security program and practices.

(U) Audit Results

(U) Overall, OIG found that IBWC had implemented an information security program; however, OIG identified weaknesses that, if exploited, could significantly impact the information security program controls and expose IBWC to security breaches. The weakened security controls could also adversely affect the confidentiality, integrity, and availability of information and information systems. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, OIG determined that IBWC should address the 14 control weaknesses described.

A. (U) System Inventory

(U) As reported by OIG for FY 2011, IBWC's inventory management process to update and manage its information technology (IT) assets needed to be improved. IBWC's inventory of systems consisted of four information systems: GSS, GIS, and the SCADA systems, which are also known as Industrial Control Systems. GSS and GIS are operated at the IBWC headquarters in El Paso, and the two SCADA systems are located in San Diego, and Nogales. IBWC had performed an inventory of its hardware and systems during FY 2012; however, OIG found that IBWC had not fully accounted for all IT assets. OIG determined that the IBWC inventory had listed components associated only with GSS and GIS. OIG identified components in the server room and in the wiring rooms of the first and third floors at the headquarters in El Paso, in the field office in Fort Hancock, and at the site in Las Cruces, that were not recorded in the inventory. In addition, OIG determined that IBWC had not included the SCADA systems operated at the IBWC Nogales field office and the San Diego wastewater treatment plant in the inventory listing.

(U) 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. The inventory should, also include interfaces between each system and other systems or networks not operated by or under the control of the agency.[13]

(U) IBWC officials stated that they were unaware of the FISMA requirement to update the system inventory when hardware changes occurred. Without a full system inventory of IT

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

assets, including the SCADA systems and changes to assets, IBWC did not have an accurate accounting of all related system interfaces or underlying support systems and was not able to properly identify and mitigate security risks. As a result, critical management processes such as strategic planning, budgeting, system administration, patch management, and resource management, could be adversely affected.

> **(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) Management Response:** IBWC concurred with the recommendation, stating that its "Information Management Division (IMD) is implementing a comprehensive IT asset inventory to fully account for all IT assets" within the GSS (and Major application GIS), SBIWTP Veolia, SBIWTP SCADA, and Nogales SCADA.
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has conducted a complete inventory of all IBWC IT assets.
>
> **(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) Management Response:** IBWC concurred with the recommendation, stating that "an IBWC System inventory was completed in 2012" and that it would "be conducting an annual inventory of all four systems in 2013." IBWC further stated that the process for conducting these inventories was being developed.
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has completed an annual inventory of all IBWC IT assets.

B. (U) Risk Management Program

(U) As reported by OIG for FY 2011, IBWC had not implemented a risk management framework to include information security policies and procedures that describe the roles and responsibilities of key participants at the organization and system levels. OIG determined that IBWC had not taken corrective actions to develop a risk management framework and did not have a governance structure in place to determine whether IBWC had effectively managed information security risk. As stated in NIST SP 800-37, Revision 1,[14] the risk management

[14] **(U)** NIST SP 800-37, rev.1, "Guide for Applying the Risk Management Framework to Federal Information Systems" - 2.1 "Integrated Organization-Wide Risk Management," Feb. 2010.

framework is essential to IBWC because it addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy.

(U) In addition, IBWC had not developed an IT strategic plan or enterprise architecture that showed the IT goals for the organization or linked the strategic goals and objectives to the defined business functions. An IBWC official stated that IBWC had planned to incorporate its IT strategic plan funding requirements into the FY 2014 organizational budget request which is under development and would include all IBWC IT security investments. NIST SP 800-37[15] states that it is essential to prioritize "missions and business processes with respect to the goals and objectives of the organization.

(U) Without the implementation of the risk management strategy at the organizational level, operations at the system level could be negatively affected. Specifically, management may be unaware of existing security vulnerabilities, and associated funding allocations may not be adequately determined to address those vulnerabilities.

~~(SBU~~) At the information system level, IBWC had not completed the Security Assessment Authorization package as required by NIST SP 800-82[16] and NIST SP 800-53, Revision 3[17] for any of its three systems. Specifically, OIG determined the following weaknesses in the risk management program:

- **~~(SBU)~~** The GSS Authorization to Operate had expired, and no Authorization to Operate existed for GIS and the SCADA systems. An Authorization to Operate provides verification that an authorizing official has accepted identified risks with the systems. According to an IBWC official, all systems were in the production environment.
- **~~(SBU)~~** Risk assessments, as required by NIST SP 800-37, Revision 1,[18] had not been conducted for GSS, GIS, and the SCADA systems. However, site assessments for the SCADA systems were performed for Nogales and San Diego.
- **~~(SBU)~~** The GSS System Security Plan was being updated to reflect the changes that had occurred since the last System Security Plan was certified by the Chief Information Officer in April 2007. A System Security Plan had not been completed for GIS and the SCADA systems.
- **~~(SBU)~~** For all four systems, IBWC did not perform a Security Test and Evaluation, which is a security assessment report supporting the independent assessor's evaluation of management, operational, and technical controls.

[15] **(U)** Ibid.

[16] **(U)** NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," sec. 6.1.1, "Security Assessment and Authorization," June 2011.

[17] **(U)** NIST SP 800-53, rev. 3: "CA-2 Security Assessments," "CA-6 Security Authorization," and "SA-11 Developer Security Testing," Aug. 2009 (last updated May 2010).

[18] **(U)** NIST SP 800-37, rev.1, "Guide for Applying the Risk Management Framework to Federal Information Systems," sec. 3.5, "RMF Step 5 - Authorize Information System," Feb. 2010.

(U) IBWC had not effectively followed guidelines contained in NIST SP 800-37, Revision 1,[19] for completion of the security assessment and authorization packages. An IBWC official stated that IBWC was unaware of the NIST requirement to complete the security assessments and authorization package for the GIS system. Further, the IBWC official stated that the requirement for updating GSS and the SCADA systems had not been completed because of a lack of available resources. Without a security assessment and authorization in place, IBWC's risk management framework has been weakened and IBWC does not have the ability to assess, address, and monitor information security risk.

> **(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) Management Response:** IBWC concurred with the recommendation, stating that a draft form of the risk management framework policy and procedure was available and that staff would internally review the draft by November 30, 2012.
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has reviewed and approved the risk management framework policy and procedure.
>
> **(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.
>
> ~~(SBU)~~ **Management Response:** IBWC agreed with the recommendation, stating that an updated System Security Plan for the GSS system was available for review and the System Architecture and Design Requirements documentation would be used to help create the System Security Plan required for GIS before it goes into full production. IBWC also stated that it was reviewing upgrades to the systems specified.
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC developed, tested, and obtained management approval of the security documents specified.
>
> ~~(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

[19] **(U)** NIST SP 800-53, rev. 3, "CA-2 Security Assessments, CA-6 Security Authorization, RA-3 Risk Assessment" Aug. 2009 (last updated May 2010).

required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 3 and NIST SP 800-82.

(U) Management Response: IBWC concurred with the recommendation, stating that IMD would "develop the necessary security assessments and authorization packages for the GIS and SCADA systems and update the GSS authorization package as part of FY 2013 priorities."

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC developed, tested, and obtained management approval for the security documents as required.

(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) Management Response: IBWC concurred with the recommendation, stating that the risk management framework draft being reviewed "provides a specific time frame for the Assessment and Authorization (A&A) processes" and for "the regular update and acceptance of System Security plans and Security Assessments."

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed, tested, and obtained management approval of the security documents as required.

(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) Management Response: IBWC concurred with the recommendation, stating that it is conducting "a risk assessment and pen test" on its GSS system.

~~(SBU)~~ OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed, tested, and obtained management approval of the security documents as required.

C. (U) Configuration Management

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not implemented effective CM policy and procedures for its IT environment. Although IBWC had CM policy and procedures in place, IBWC had not accounted for the patch management process to evaluate and approve patches for application, installation, oversight, and review of the patch status on the systems. OIG determined that responsibility for the implementation of configuration changes and updates to the baseline configuration for the systems, operating systems, databases, network, and patch installation was distributed among the various IT personnel without controls to ensure compliance as required by NIST SP 800-53, Revision 3.[20] Specifically, OIG determined that IBWC had not implemented a change control process that involves the systematic proposal, justification, implementation, test, evaluation, review, and disposition of changes to the system, including upgrades and modifications. Further, IBWC had not maintained control over all hardware connected to its SCADA system at the San Diego wastewater treatment plant, which is operated by contractors.

(U) According to NIST SP 800-53, Revision 3,[21] "security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information."

(U) This guidance states that organizations should develop and maintain a "formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance" with documented procedures for implementation of the policy that an organization should review, approve, document, audit, and provide oversight for CM controls for information systems.

(U) NIST standards require that the organization report, test, and correct potential CM problems, identifies, reports, and corrects information system flaws; and incorporates flaw remediation into the organizational configuration management process.[22] NIST SP 800-40, Version 2.0, states that remediation testing guidelines indicate that patches and configuration modifications should be tested on non-production systems since remediation can easily produce unintended consequences.[23]

(U) An IBWC official stated that CM policy and procedures were currently being updated to include the patch management process. An IBWC official also stated that a test environment did not exist for testing of configuration changes and patches. Without implemented procedures that govern the performance of the CM process, IBWC may not be able to effectively manage the IT security program, which could lead to the introduction of security weaknesses and inconsistent performance.

[20] **(U)** NIST SP 800-53, rev. 3, CM-1 "Configuration Management Policy and Procedure," CM-2 "Baseline Configurations," CM-3 "Configuration Change Control," CM-4 "Security Impact Analysis," and CM-5 "Access Restrictions for Change" Aug. 2009 (last updated May 2010).
[21] **(U)** NIST SP 800-53, rev. 3, ch. 1, "Introduction," Aug. 2009 (last updated May 2010).
[22] **(U)** NIST SP 800-53, rev. 3, SI-2 "Flaw Remediation" Aug. 2009 (last updated May 2010).
[23] **(U)** NIST SP 800-40, ver. 2.0, "Creating a Patch and Vulnerability Management Program," sec. 2.6, "Testing Remediations," Nov. 2005.

(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) Management Response: IBWC concurred with the recommendation, stating that "existing procedures for patch management" are being documented and tested for inclusion in the existing CM policy and procedure and that it expects an approved update to the existing CM policy by March 2013.

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented configuration management and testing procedures as required.

(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) Management Response: IBWC concurred with the recommendation, stating that it would begin to develop similar CM policy and procedure for all systems that are part of the IBWC operations and expects to have draft policy in place by March 2013.

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented procedures for the oversight of all systems and hardware as required.

D. (U) Incident Response and Reporting

(U) OIG found that IBWC's incident response and reporting did not fully comply with provisions of NIST SP 800-53, Revision 3.[24] Specifically, IBWC had not updated its incident response policy and procedure to reflect changes made to its reporting documentation.

(U) NIST SP 800-53, Revision 3,[25] states:

(U) The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

[24] **(U)** NIST SP 800-53, rev. 3, IR-1 through IR-8, Aug. 2009 (last updated May 2010).

[25] **(U)** NIST SP 800-53, rev. 3, IR-1 "Incident Response Policy and Procedures." Aug. 2009 (last updated May 2010).

a. **(U)** A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. **(U)** Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

(U) An IBWC official stated that the incident report template had been updated but that the template had not been incorporated in the incident response and reporting procedures. The lack of updated procedures may prevent IBWC from reporting security incidents to appropriate authorities.

> **(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) Management Response:** IBWC concurred with the recommendation, stating that an updated incident report template has been uploaded to the "existing draft Incident Response Policy & Procedures . . . being updated to the new directives format initiated by IBWC" and that the draft would be "completed, reviewed, and staffed by December 2012 for re-approval by the Commissioner."
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has incorporated the updated incident report template into the incident response and reporting procedures and that it periodically assesses compliance with the procedures as required.

E. (U) Security Training

(U) As reported by OIG for FY 2011, IBWC had not trained all employees and contractors as required by its security awareness training program. IBWC developed a draft security awareness training policy and procedures that included sanctions for employees who failed to take and complete IT security awareness training. OIG determined that IBWC employees had not completed the required security awareness training and that not all employees with significant security responsibilities had completed their specialized training, as of April 27, 2012. When OIG completed on-site verification in April 2012, IBWC had not started its annual training of employees and contractors. No IBWC employees or contractors had completed the required annual training; however, at that time, 5 months remained in the fiscal year during which IBWC staff could have completed the training. Although IBWC's security awareness training program required all personnel to complete annual security awareness training and users with significant security responsibilities to complete specialized training, OIG determined that IBWC did not require new employees to complete initial security awareness training prior to accessing information systems, as required by NIST SP 800-53, Revision 3.[26]

[26] **(U)** NIST SP 800-53, rev. 3, AT-2 "Security Awareness," Aug. 2009 (last updated May 2010).

(U) OMB Circular No. A-130 states "The Computer Security Act requires Federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency."[27] Training ensures that all users are knowledgeable of the rules of the system.[28] Although IBWC had acquired a security awareness training product in April 2012, an IBWC official stated that the product had not been implemented because of the limited number of staff assigned to the Information Management Division (IMD) to support the security training program. However, IBWC officials stated that IBWC intends to administer security awareness training to all employees, including those with significant security responsibilities by the end of the fiscal year.

(U) Regarding the necessity for annual security training, NIST SP 800-50[29] states:

> **(U)** [A]t a minimum, the entire workforce should be exposed to awareness material annually. A continuous awareness program, using various methods of delivery throughout the year, can be very effective. Security training for groups of users with significant security responsibility (e.g., system and network administrators, managers, security officers) should be incorporated into ongoing functional training as needed.

(U) NIST SP 800-53, Revision 3,[30] also supports training requirements and related corrective actions: "The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes and [Assignment: organization-defined frequency] thereafter." Further, NIST SP 800-53, Revision 3,[31] states, "[T]he organization [should employ] a formal sanctions process for personnel failing to comply with established information security policies and procedures."

(U) Without the completion of initial and annual security awareness training, personnel may be unaware of risks that may compromise the confidentiality, integrity, and availability of data. As a result, personnel may be unable to recognize and respond appropriately to security concerns. Employees with significant security responsibilities who are not properly trained create a risk for IBWC since they may introduce vulnerabilities because of their elevated level of system permissions.

> **(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

[27] **(U)** OMB Circular No. A-130, revised, "*Management of Federal Information Resources,*" app. III, "Security of Federal Automated Information Resources." – B. "Descriptive Information," a. "General Support Systems," 2.b "Training."

[28] **(U)** OMB Circular No. A-130, revised, A. "Requirements," 3.a.2.b "Training."

[29] **(U)** NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," pg.20, F/N 13, Oct. 2003.

[30] **(U)** NIST SP 800-53, rev. 3, AT-2 "Security Awareness," Aug. 2009 (last updated May 2010).

[31] **(U)** NIST SP 800-53, rev. 3, PS-8 "Personnel Sanctions," Aug. 2009 (last updated May 2010).

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) Management Response: IBWC concurred with the recommendation, stating that IMD had updated its existing Security Awareness Training policy and procedure to include the requirements described and that the policy will be "reviewed, reformatted and staffed for review and sent for approval by December 2013."

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that the security awareness training policy described is finalized and that personnel take the training before they are granted access to information technology systems as required.

(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.

~~(SBU)~~ Management Response: IBWC concurred with the recommendation, stating that the draft Security Awareness Training policy and procedure "addresses disciplinary and corrective action the IMD will be authorized to impose on personnel that do not comply with this requirement." IBWC also provided information on the status of personnel enrolled in the training and stated that notifications had been issued to "non-compliant employees and their supervisors" and that additional notification "would be issued for noncompliance."

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that all IBWC personnel attend security awareness refresher training and that access to information technology systems and assets is suspended for personnel who do not successfully complete the training as required.

(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.

~~(SBU)~~ Management Response: IBWC concurred with the recommendation, stating that the updated policy and procedure "addresses this requirement and budgetary requirements to ensure the required training occurs" annually. IBWC further stated that all seven IBWC personnel with significant IT responsibilities have completed training.

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that the specialized security training requirement has been met as required.

F. (U) Plan of Action and Milestones

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not fully implemented an effective POA&M process. Since OIG's last review, IBWC had made improvements in its POA&M process by including details of the estimated resource requirements and corrective action plans to close the POA&M deficiencies, as required in the OMB template. In addition, IBWC had used the POA&M for developing, maintaining, and reporting the IBWC's planned actions for identified weaknesses related to GSS. However, IBWC had not determined the security weaknesses for GIS and the SCADA systems because IBWC had not completed the necessary security documents identifying the security controls in place and those that require improvement. System security plans and an independent assessment (Security Test and Evaluation report) would identify the controls that were in place and those that were either missing or deficient (were not up to the standard required by the FIPS 199[32] levels of potential impact on organizations associated with the system). The absence of these security documents indicated that IBWC had not conducted the necessary testing of GIS and the SCADA systems; therefore, IBWC was unable to identify the weaknesses requiring remediation. Additionally, IBWC was conducting periodic security scans of GSS, but the weaknesses identified in those scans were not recorded in the POA&Ms. OIG identified the following deficiencies:

- **(U)** The POA&Ms were not properly updated and provided to the Chief Information Officer on a quarterly basis.
- **~~(SBU)~~** The POA&Ms did not include findings identified from GSS vulnerability scan assessments, as well as vulnerabilities associated with the SCADA systems identified from site assessments.
- **(U)** The POA&Ms did not include a specific corrective action plan for completing the security assessment and authorization package for GSS, GIS, and the Nogales SCADA system.
- **(U)** The documentation for the corrective action activities was not maintained.
- **(U)** The POA&Ms were not reviewed on a periodic basis to ensure updates were recorded. Specifically, OIG determined that the estimated completion dates had passed, that updates were not made to the estimated completion date, and that an explanation supporting the delay was not documented.

(U) According to NIST SP 800-53, Revision 3,[33] "the organization updates existing plan of action and milestones [*Assignment: organization-defined frequency]* based on the findings

[32] **(U)** FIPS 199, Feb. 2004.
[33] **(U)** NIST SP 800-53, rev. 3, CA-5 "Plan of Action and Milestones," Aug. 2009 (last updated May 2010).

from security controls assessments, security impact analyses, and continuous monitoring activities."

(U) NIST SP 800-53, Revision 3[34] also states that "The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation."

(U) Elaborating further on the importance of thorough and effective POA&Ms, OMB Memorandum M-08-21[35] states:

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

(U) The implementation of a POA&M process is important to assess the current state of the security posture of GSS, GIS, and the SCADA systems and to aid in oversight of IT investments. IBWC conducted periodic security scans of GSS but had not accounted for the identified weaknesses in the POA&M process, which could result in POA&Ms becoming out of date. On the other hand, IBWC did not conduct any security scans or complete the security documentation for GIS and the SCADA systems and, therefore, was unable to identify existing vulnerabilities in the systems. Without inclusion of vulnerabilities and periodic updates of POA&M activities, IBWC management may be unaware of weaknesses and the status of corrective actions. As a result, delays in the implementation of corrective actions may not be appropriately identified and resolved in a timely manner.

> **(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.
>
> **~~(SBU)~~ Management Response:** IBWC concurred with the recommendation, stating that it is using its POA&M process "to develop, maintain, and report the IMD work plan" and to track progress toward closing each entry. IBWC further stated that it has entered identified weaknesses and vulnerabilities into the POA&M database "so necessary resources and manpower are allocated to address each issue," that "the recently discovered vulnerabilities" are being prioritized and scheduled for remediation, and that employees have been notified that regular update and maintenance of the database is now considered "a measurable performance element that will affect their annual performance ratings."

[34] **(U)** NIST SP 800-53, rev. 3, PM-4 "Plan of Action and Milestones Process," Aug. 2009 (last updated May 2010).
[35] **(U)** OMB Memorandum M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," July 14, 2008.

~~(SBU)~~ OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has implemented a POA&M process, including vulnerabilities identified from all sources, and updated milestone dates as required.

G. (U) Remote Access

(U) As reported by OIG for FY 2011, IBWC had not finalized and implemented its remote access policy and procedure to comply with NIST requirements. An IBWC official stated that the access control policy and procedure document contains procedures for remote access, but OIG determined that the procedures still require review and formal approval by IBWC management. During fieldwork completed in 2012, OIG identified additional weaknesses in remote access and wireless devices.

(b) (5)

[redacted]

[36] **(U)** OMB Memorandum M-06-16, “Protection of Sensitive Agency Information,” June 23, 2006.
[37] **(U)** NIST SP 800-53, rev. 3, AC-17 “Remote Access,” Aug. 2009 (last updated May 2010).
[38] **(U)** OMB Memorandum M-06-16.

(U) Wireless Access Weaknesses

(SBU) OIG determined that IBWC did not have a wireless policy and procedure in place (b) (5) [redacted]

~~**(SBU)**~~ OIG identified that IBWC had one wireless access point that IBWC management had requested. An IBWC official stated that only portable devices configured by IMD could have connected to the wireless access point. IBWC configured and issued 11 iPads and two laptops for authorized use within the IMD office to connect to the wireless access point. (b) (5) [redacted] OIG determined that IBWC had not periodically reviewed unauthorized access to the wireless network. NIST SP 800-53, Revision 3,[40] states:

> **(U)** The organization:
>
> **(U)** a. Establishes usage restrictions and implementation guidance for wireless access;
> **(U)** b. Monitors for unauthorized wireless access to the information system;
> **(U)** c. Authorizes wireless access to the information system prior to connection; and
> **(U)** d. Enforces requirements for wireless connections to the information system.

(b) (5) [redacted]

(U) Inadequate remote access controls increased the risk that accounts may have been accessed and used by individuals to perform unauthorized activities. Without proper controls in place, unauthorized activities could occur without timely detection, which could adversely impact confidentiality, integrity, and availability of the data.

> **(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) Management Response:** IBWC concurred with the recommendation, stating that the access control policy and procedure is being updated and would be "ready for review and final approval" by the Commissioner in December 2013.

[39] **(U)** As defined in NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems," July 2008, Media Access Control addresses are hardware addresses that "uniquely identify each component of an IEEE [Institute of Electrical and Electronics Engineers] 802-based network."

[40] **(U)** NIST SP 800-53, rev. 3, AC-18 "Wireless Access," Aug. 2009 (last updated May 2010).

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has finalized and implemented remote access policy and procedure as required.

~~(SBU)~~ **Recommendation 16.** OIG recommends that the Chief Information Officer implement remote access controls that is enforced (b) (5) [redacted]

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that a "solution to address the lack of full disk encryption on all IBWC issued laptops was purchased in FY 2012." IBWC further stated that it is conducting a "complete inventory and recall of all laptops" that will require the return of all laptops to headquarters for software implementation and update. (b) (5) [redacted]

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has implemented remote access controls enforced (b) (5) [redacted]

(U) 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) Management Response. IBWC concurred with the recommendation, stating that IMD would "include wireless policy and procedures in the existing update" to access control policy and procedure to address usage restrictions, access procedures, authorization monitors, and compliance requirements for wireless access and connections to the GSS. IBWC further stated that only one wireless access point exists within IBWC headquarters and that existing documentation has been updated.

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented a wireless policy and procedure as required.

H. (U) Identity and Access Management

(U) OIG identified three areas of weakness in the identity and access management process; using e-authentication process, monitoring IT personnel with privileged permissions, and obtaining signed Rules of Behaviors agreements from information systems users.

(U) Using the E-authentication Process

~~(SBU)~~ E-authentication is the process of establishing confidence in the identities of users attempting to electronically access an information system.[41] Although IBWC had implemented Identification and Authentication Policy and Procedure, OIG found that the policy had not been reviewed or updated since 2009.

(U) OMB Memorandum M-04-04[42] identifies a five-step process by which agencies should meet their e-authentication assurance requirements:

- **(U)** Conduct a risk assessment of the government system.
- **(U)** Map identified risks to the appropriate assurance level.
- **(U)** Select technology based on e-authentication technical guidance.
- **(U)** Validate that the implemented system has met the required assurance level.
- **(U)** Periodically reassess the system to determine technology refresh requirements.

(U) In addition, NIST SP 800-53, Revision 3,[43] states that organizations should review and update the following:

a. **(U)** A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. **(U)** Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

~~(SBU)~~ OIG determined that personal identity verification cards had been configured to the network prior to any testing or assessment performed, as required by OMB Memorandum M-04-04,[44] and individuals had the ability and had been using their personal identity verification cards to access the network. However, an IBWC official stated that no formal risk assessment was performed prior to the implementation of the personal identity verification card because IBWC was not aware that a risk assessment was required. Without an effective e-authentication process, the control designed to identify systems users' identities could be compromised.

(U) Monitoring Information Technology Personnel With Privileged Permissions

~~(SBU)~~ IBWC possesses the capability of tracking and logging administrative activities; however, OIG found that IBWC did not have a formal process in place for tracking and

[41] **(U)** OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," Dec. 16, 2003.
[42] **(U)** Ibid.
[43] **(U)** NIST SP 800-53, rev. 3, IA-1 "Identification and Authentication Policy and Procedures," Aug. 2009 (last updated May 2010).
[44] **(U)** OMB Memorandum M-04-04, Dec. 16, 2003.

monitoring users with privileged role assignments and that management had not established a process for monitoring users with privileged permissions. NIST SP 800-53, Revision 3,[45] states:

> **(U)** The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

(U) When users with privileged permissions are not monitored, unauthorized activities could harm the IBWC information assets and adversely affect the confidentiality, integrity and availability of data.

(U) Obtaining Signed Rules of Behavior Agreements From Information Systems Users

(U) OIG found that IMD had generated a network account and temporary password prior to user application for network access. IBWC officials stated that users did not receive login credentials until Rules of Behavior agreements had been signed by the users and Information Systems Security Officer. OIG found that four (33 percent) of 12 (100 percent of new users for the audit period) Rules of Behavior agreements were not signed by the Information System Security Officer. NIST SP 800-53[46] requires users to read and sign Rules of Behavior documents. The Information System Security Officer stated he was not available to sign the four Rules of Behavior documents identified by OIG as lacking appropriate signature.

> **(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) Management Response:** IBWC concurred with the recommendation, stating that IMD was updating the existing identification and authentication policy and procedure to comply with new IBWC directives and include specific language and procedures that would require verification of users' signatures by ISSOs on all Rules of Behavior documents before initial user credentials are issued.
>
> **(U) OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has updated and implemented identification and authentication management procedures to include e-authentication procedures as required.

[45] **(U)** NIST SP 800-53, rev. 3, AC-6 "Least Privilege," Aug. 2009 (last updated May 2010).

[46] **(U)** NIST SP 800-53, rev. 3, PL-4 "Rules of Behavior," Aug. 2009 (last updated May 2010).

(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) Management Response: IBWC concurred with the recommendation, stating that IMD was creating documentation on required risk assessments and testing before implementing any new technology or access to services required by the agency.

~~(SBU)~~ OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has performed a risk assessment identifying the risks to system security as required.

I. (U) Continuous Monitoring

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not fully implemented a continuous monitoring program for its IT systems. During the FY 2012 audit, OIG identified three weaknesses in the IBWC continuous monitoring process: (b) (5) [redacted] An IBWC official stated that there are no documented policies and procedures detailing the strategy and plans for conducting continuous monitoring activities that include routine vulnerability scanning, log monitoring, and notification of unauthorized devices due to limited resources.

(U) Formal Continuous Monitoring Process

~~(SBU)~~ OIG determined that IBWC had assessed and installed a vulnerability management tool designed to perform automated routine security assessments of its system environment to address this deficiency. (b) (5) [redacted]

(b) (5) [redacted]

(U) NIST SP 800-53, Revision 3,[47] states:

> **(U)** The organization subsequently initiates specific follow-on actions as part of a comprehensive continuous monitoring program. The continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation. In particular, the organization revisits on a regular basis, the risk management activities described in the Risk Management Framework. In addition to the ongoing activities associated with the implementation of the Risk Management Framework, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls.

(U) When such events occur, organizations, at a minimum, should take the following actions:

- **(U)** Reconfirm the security category and impact level of the information system.
- **(U)** Assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.
- **(U)** Plan for and initiate any necessary corrective actions.

> **(U)** After the security controls and/or control upgrades have been implemented and any other weaknesses or deficiencies corrected, the controls are assessed for effectiveness to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. If necessary, the security plan is updated to reflect any additional corrective actions taken by the organization to mitigate risk.[48]

(U) Further, the NIST publication defines security assessment requirements to include the establishment, implementation, maintenance, and reporting of a continuous monitoring program for information systems. Additional NIST guidance outlines monitoring and detection requirements in accordance with applicable legislation, regulations, and executive policy.[49]

(U) NIST SP 800-53, Revision 3,[50] states that the organization "scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency*

[47] **(U)** NIST SP 800-53, rev. 3, sec. 3.4 "Monitoring Security Controls," Aug. 2009 (last updated May 2010).
[48] **(U)** Ibid.
[49] **(U)** NIST SP 800-53, rev. 3, SI-4 "Information System Monitoring," Aug. 2009 (last updated May 2010).
[50] **(U)** NIST SP 800-53, rev. 3, RA-5 "Vulnerability Scanning," Aug. 2009 (last updated May 2010).

and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported."

(U) Without periodic reviews or the performance of risk-based security assessments, new threats and vulnerabilities may not be identified and mitigated in a timely manner, potentially causing damage or disruption to IBWC information systems.

(U) Vulnerability Scan Results

(~~SBU~~) OIG determined that identified vulnerabilities had not been included within the POA&Ms tracking database and that the firewall logs had not been reviewed. Also, IBWC had not performed the Security Test and Evaluations necessary to verify compliance with its security policy guidelines and to evaluate the effectiveness of the security controls against anticipated threats for GSS, GIS, and the SCADA systems. The Information Systems Security Officer had not provided the scan results to the IBWC official responsible for maintaining the POA&M database because of unfamiliarity with the process. OMB Memorandum M-08-21[51] states:

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

(U) When vulnerabilities were not reported to the POA&M database, IBWC did not have an effective process to determine corrective action and security risk exposure. (Additional details are addressed in Finding F – Plans of Action and Milestones of this report.)

(U) Supervisory Control and Data Acquisition Systems Monitoring Processes

(~~SBU~~) In addition to apparent challenges in performing automated vulnerability scans and reviews, OIG found that the SCADA control centers at the San Diego wastewater treatment plant are not effectively monitored to identify and mitigate security incidents. An IBWC contractor stated that screens had not always been monitored for incidents such as alarms despite the fact that SCADA systems are designed to collect field information, transfer information to a central computer facility, and display, graphically or textually, information, allowing operators to monitor or control an entire system from a central location in real time. NIST SP 800-53 states that personnel are required to report suspected security incidents to the organizational incident response capability and to report "security incident information to designated authorities" within an acceptable timeframe defined by the organization.[52] Without regular security monitoring, incidents could go unnoticed, potentially leading to additional damage and/or disruption. IBWC

[51] **(U)** OMB Memorandum M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," dated July 14, 2008.

[52] **(U)** NIST SP 800-53, rev. 3, IR-6 "Incident Reporting," Aug. 2009 (last updated May 2010).

also needed to conduct regular security monitoring to identify problems with security controls, such as misconfigurations and failures.

> ~~(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.
>
> ~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that IMD was developing policies and procedures to assist in the full implementation of an effective continuous monitoring program for its IT systems and that IMD had received approval for a permanent, part-time employee whose main responsibility would be "many of the tasks required to maintain a continuous monitoring program."
>
> ~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented policies and procedures to perform continuous monitoring to include automated routine vulnerability assessments for the systems specified. The results of such security assessments should be reviewed, and POA&Ms should be developed for the improvement of the security controls of major systems as required.

J. (U) Contingency Planning

(U) As reported by OIG for FY 2011, IBWC's contingency planning process required significant improvements. An effective contingency planning program is "designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability."[53] NIST SP 800-34, Revision 1,[54] states that information systems are "vital elements" in most business functions and that "it is critical" that the services provided by these systems be able to operate effectively without excessive interruption. NIST guidance further states, "Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Although IBWC had documented a contingency plan for the GSS and had configured an automated back-up process for the headquarters and field offices, OIG identified the following deficiencies:

(b) (5) [redacted]

[53] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," ch. 2 – "Background," May 2010.

[54] **(U)** NIST SP 800-34, rev. 1, ch. 1 – "Introduction," May 2010.

(b) (5)
[redacted]

(U) IBWC is required by NIST SP 800-34[55] to have a collection of plans to prepare for response, continuity, recovery, and resumption of mission and/or business processes and information systems in the event of a disruption. OIG determined that a Business Impact Assessment, which helps to identify and prioritize critical IT systems and components, had not been performed. IBWC management stated that limited resources had prevented them from completing the contingency planning documentation. Without a Business Impact Assessment, IBWC could not identify the critical Business Processes of IBWC to generate a proper Business Continuity/Recovery Plan.

(b) (5)
[redacted]

[55] **(U)** NIST SP 800-34, rev. 1, app. C, "Response to Question 2," May 2010.
[56] **(U)** NIST SP 800-34, rev. 1, ch. 3, "Information System Contingency Planning Process," May 2010.
[57] **(U)** NIST SP 800-82, "Guide to Industrial Control Systems Security (ICS)," sec. 6.2.3.1 "Business Continuity Planning," June 2011.
[58] **(U)** NIST SP 800-53, rev. 3, CP-6"Alternate Storage Site," Aug. 2009 (last updated May 2010).
[59] **(U)** According to NIST SP 800-12, "An Introduction to Computer Security – The NIST Handbook," a hot site is "a building already equipped with processing capability and other services and a cold site houses processors that can be easily adapted for use."

(b) (5)

[redacted]

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented contingency planning procedures and conducted testing for operational effectiveness of all major systems as required.

~~(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.

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that IMD had awarded a contract in September "to assist with the implementation of a VMWare and Cisco Virtualization solution with Citrix" for secure web access for a disaster recovery system at the Las Cruces continuity of operations site. IBWC further stated that this solution would "serve as a centralized backup of hardware, software, and data, which would be shared across all IBWC divisions and accessible by authorized IBWC personnel during a disaster recovery."

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has finalized the continuity of operations site and conducted testing for operational effectiveness of all major systems as required.

K. (U) Oversight of Contractor System

~~(SBU)~~ As reported by OIG for FY 2011, IBWC had not implemented an effective oversight program for its contractor system. During fieldwork completed in 2012, OIG found that IBWC's San Diego field office had not documented policies and procedures for IBWC's oversight of systems operated by contractors and had not included the SCADA operations within IBWC's IT boundaries. OIG determined that IBWC had not developed policies and procedures to oversee the San Diego operations and that the field office had relied heavily on contractor-produced policies and procedures. The contract between IBWC and the contractor required the contractor to document a SCADA security plan and an IT Security Plan.[60] Although the SCADA security plan included an explanation of security controls, it did not explain functioning

[60] **(U)** Contract No. IBM10C0016, "Amendment of Solicitation Commercial Clauses," Question and Response 3.

controls or planned implementation for the San Diego operation. Also, the security plan did not address the security controls required by NIST SPs 800-53[61] and 800-82.[62]

~~(SBU)~~ In addition, IBWC officials did not have adequate control over the IT functions at the San Diego wastewater treatment plant or the IT assets purchased and maintained by the contractor in support of operations. An IBWC official stated that the organization was aware of the deficiencies and was working to address the issues. IBWC is developing a contract modification with the San Diego contractor to include, but not be limited to, the contractor notifying IBWC of purchases. Additionally, contractor-owned software was operating on the local area network at the San Diego wastewater treatment plant without proper review and approval by IBWC's IMD.

(U) Department of Homeland Security FY 2012 Inspector General metrics publication[63] states: Contractor systems should have "documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud." "Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines."

~~(SBU)~~ Without adequate contractor oversight, IBWC cannot be assured contractor personnel are compliant with FISMA, OMB requirements, and NIST standards. Further, because IMD did not have a review and approval process in place, contractors could purchase IT assets that may not be in the best interest of IBWC. Finally, without proper oversight, there is an increased risk that data collected, processed, and maintained is exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

> **(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.
>
> ~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it has established "modifications to existing contracts" with contracted personnel at the San Diego wastewater treatment plant and was reviewing upgrade recommendations resulting from its onsite assessment in early 2012. IBWC further stated that policy and procedure detailing IBWC's oversight of contractor-operated systems would be created and developed for both the San Diego SCADA and Veolia Systems to replace existing contractor-developed policy and procedure and that the San Diego SCADA system would

[61] **(U)** NIST SP 800-53, rev. 3, Aug. 2009 (last updated May 2010).
[62] **(U)** NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," June 2011.
[63] **(U)** Department of Homeland Security, "FY2012 Inspector General Federal Information Security Management Act Reporting Metrics," sec. 10, "Contractor Systems," Mar. 6, 2012.

undergo a major upgrade in 2013 to address password and physical access issues and to remove the connection between the Veolia and SCADA Systems.

(U) OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that IMD is responsible for the oversight of information technology assets purchased and maintained by the contractor in support of operations at the San Diego wastewater treatment plant as required.

(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.

~~(SBU)~~ Management Response: IBWC concurred with the recommendation, stating the currently proposed software upgrade of the existing SBIWTP SCADA system is being reviewed before it was procured and that this action was "evidence that an approval process is in place." IBWC further stated, "Mods to the existing contract currently reflect this change."

~~(SBU)~~ OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that its IMD has reviewed and approved software before it is installed on IBWC assets as required.

L. (U) Security Capital Planning

(U) In FY 2011, OIG reported that information security costs were not integrated into IBWC's Capital Planning and Investment Control process. During recent audit fieldwork, OIG found that IBWC still had not provided OMB with a detailed explanation for major investments related to its projected IT security expenditures. An IBWC official stated that IBWC did not provide OMB with a detailed explanation of IT security expenses because IBWC is a small organization and its budget requirements are not large enough to report to OMB. According to OIG's FY 2011 report, IBWC had not always considered SCADA systems, valued at $2 million, as part of its total IT security assets to meet OMB's reporting threshold. However, another IBWC official stated that IBWC's total IT security assets, if SCADA systems are included, are valued at approximately $2.5 million, well above IBWC's estimation of OMB's $2 million reporting threshold. Further, an IBWC official stated that POA&Ms are currently being used to identify and incorporate high-priority tasks into the FY 2014 organizational budget request. However, the POA&M and capital planning request processes differ and are managed by two different positions, requiring close coordination and integration of the two processes to achieve accurate and effective requests for IT funding. (Details are addressed in Finding F – Plans of Action and Milestones of this report)

(U) IBWC had neither developed the enterprise architecture nor integrated the IT strategic plan into the budget process as part of the risk management program. Since the enterprise architecture and the strategic plan were not considered in the risk management program, IBWC may not be requesting funding levels appropriate to the risk exposure. As part of the IBWC capital planning request, an IBWC official stated that the POA&Ms were used to identify high priority tasks to improve the IT environment.

(U) To ensure appropriate allocation of resources to meet IT security projected costs, NIST guidance states that an organization "determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process" [64] and "ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement." To support security investments NIST guidance states that organizations should use "a business case/Exhibit 300/Exhibit 53 to record the resources required."[65]

(U) Without effective integration of the POA&M and capital planning request processes or a well-defined enterprise architecture and IT strategic plan, IT funding prioritizations may be negatively affected. Inadequate planning increases the risk that requests for IT security funding investments will not receive proper consideration.

> **(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) Management Response.** IBWC concurred with the recommendation, stating that it will incorporate costs of IT assets in future budget submissions once all IT assets and system inventories are finalized, which is consistent with OMB guidance.
>
> **(U) OIG Reply.** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured 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 OMB.

M. (U) Personnel Security

(U) IBWC had developed its personnel security program but needs to continue making improvements to its implementation of the program to address weaknesses reported by OIG in FY 2011. OIG determined that overall progress had been made toward the implementation of an effective personnel security program. Specifically, OIG identified that IBWC had developed a tracking mechanism to maintain and provide the status of employees who have been cleared or

[64] **(U)** NIST SP 800-53, rev. 3, SA-2 "Allocation of Resources," Aug. 2009 (last updated May 2010).

[65] **(U)** NIST SP 800-53, rev. 3, PM-3 "Information Security Resources," Aug. 2009 (last updated May 2010).

still require suitability investigation. IBWC had also made progress in completing suitability clearances for employees and contractors.

~~(SBU)~~ However, IBWC IMD staff that is responsible for the IT security functions have a "high- risk" position level and, per IBWC personnel security procedures, should have a higher level investigation requirement. OIG determined that IT personnel investigation requirements had been updated from a National Agency Check with Inquiries to Background Investigation based on IBWC revised personnel security policy and procedure. "National Agency Check and Inquiries is the basic and minimum investigation required on all new Federal employees. It consists of a National Agency Check[66] including written inquiries and searches of records covering specific areas of a person's background during the past 5 years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities." "A Background Investigation is a more in-depth version of the Limited Background Investigation[67] because the personal investigation covers the most recent 5–7 years. This investigation is required of those going into highest risk public trust positions."

(U) OIG identified the following deficiencies:

- **~~(SBU)~~** Three of 21 IBWC contractors at the San Diego wastewater treatment plant had not obtained their suitability adjudication, and the remaining 18 contractors that had received their suitability clearance had not obtained their badges in accordance with Homeland Security Presidential Directive 12.[68] Homeland Security Presidential Directive 12, Policies for a Common Identification Standard for Federal Employees and Contractors, requires background investigations to be conducted on all Federal and contractor employees.

- **~~(SBU)~~** IBWC had 23 employees with access to the IMD working space. Of the 23, only seven are assigned to IMD, and IBWC management determined that six of the employees require a higher level background investigation because of their access to IBWC systems. IBWC had initiated the process of obtaining the higher level investigations for the six employees.

(U) An IBWC official stated that completing the review process is still ongoing because of limited resources. Without fully investigating an employee's background followed by the adjudication process and subsequent clearance, there is a potential that IBWC employs personnel who are not appropriate for the position to which they have been entrusted. In addition, employees may be granted inappropriate administrator permissions to access IBWC information

[66] **(U)** A National Agency Check and Inquiries (NAC) is an integral part of all background investigations; the NAC consists of searches of Office of Personnel Management's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the Federal Bureau of Investigation Identification Division's name and fingerprint files, and other files or indices, as necessary.

[67] **(U)** A Limited Background Investigation consists of a National Agency Check and Inquiries, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent 3 years.

[68] **(U)** Homeland Security Presidential Directive-12, Policies for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004

technology and physical assets. This security weakness could also potentially impact the Department of State (Department) because the Department had placed OpenNet[69] terminals in IBWC workspaces.

(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.

~~(SBU)~~ Management Response. IBWC concurred with the recommendation, stating that it had "initiated background investigations" on all 21 contractors, that 16 investigations had been "completed and adjudicated," and that the remaining two investigations "are still 'open' pending completion of investigative leads." IBWC further that stated that 11 contractors had been issued appropriate credentials as required and that the remaining contractors "are pending appointments at credentialing centers."

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has finalized its contractors' suitability clearances, including formal clearance adjudication, and issued badges, as required.

(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) Management Response: IBWC concurred with the recommendation, stating that background investigations on all IT personnel had been completed.

~~(SBU)~~ OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has ensured that the adjudication process has been completed for the IT employees undergoing background investigations.

N. (U) Physical and Environmental Protection

~~(SBU)~~ As reported by OIG for FY 2011, physical and environmental protection controls of organizational assets remained a challenge. IBWC could significantly strengthen physical and environmental protection of organizational assets by improving physical access controls, securing SCADA control centers and servers, limiting access to server rooms and equipment, and addressing environmental protection weaknesses as outlined in NIST guidance. (b) (5) [redacted]

[69] **(U)** OpenNet is the Department of State's internal network (intranet), providing access to State-specific Web pages, e-mail, and other resources. Only authorized personnel who meet 12 FAM 621.1a are allowed access to OpenNet.

(b) (5)

(U) Physical Protection Weaknesses

~~(SBU)~~ While examining physical access controls, OIG found that IBWC should make improvements to protect systems from unauthorized access that could compromise the confidentiality, integrity, and availability of data. IBWC had made progress since FY 2011 by implementing a manual log process for IBWC San Diego contractors to account for the entry and exit of Mexican trucks through the international boundary gate. According to physical access authorizations outlined in NIST guidance,[70] organizations should establish, review, and maintain current lists of employees and contractors with authorized facility access and administer appropriate corresponding credentials.

(U) Physical Access Devices

(b) (5)

(U) Proximity Access Cards

~~(SBU)~~ The proximity access cards were controlled by the contractors who are located at the wastewater treatment plant. (b) (5)

(U) Remote Gate Devices

(SBU) The remote gate devices are accessible to the San Diego IBWC employees and contractors. (b) (5)

[70] **(U)** NIST SP 800-53, rev. 3, PE-2 “Physical Access Authorization,” Aug. 2009 (last updated May 2010).

(b) (5) [redacted]

(U) According to NIST SP 800-53, Revision 3,[71] "the organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible), issues authorization credentials, reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access." Without proper accountability for and record of remote gate devices, there is an increased risk that the devices could be used for purposes other than work related access to the San Diego wastewater treatment. An IBWC official stated that IBWC was aware of the risks associated with the number of individuals with proximity cards or remote gate devices and was in the process of identifying corrective actions to mitigate the risk.

(U) Supervisory Control and Data Acquisition Control Centers and Servers

~~(SBU)~~ OIG found that IBWC did not enforce physical access authorizations to the information system independent of the physical access controls for the facility. Although there were physical access controls in place at the wastewater treatment plant, (b) (5) [redacted]

[71] **(U)** NIST SP 800-53, rev. 3, PE-2.

[72] **(U)** According to NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," June 2011, "A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data."

[73] **(U)** According to NIST SP 800-82, a "Programmable Logic Controller is generally used for discrete control for specific applications and generally provides regulatory control."

(b) (5) [redacted]

(U) NIST SP 800-82[74] states:

- **(U)** Restricting physical access to the [Industrial Control System] network and devices. Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.

- **(U)** Protecting individual ICS components from exploitation. This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.

(U) Unauthorized access to network devices and administrative functions could allow a user to disrupt Industrial Control Systems operations or monitor Industrial Control Systems network activity. Also, access to network equipment should be controlled to prevent damage or destruction. In addition, improper access to network equipment could lead to any of the following conditions:

- **(U)** Physical theft of data and hardware.
- **(U)** Physical damage or destruction of data and hardware.
- **(U)** Unauthorized changes to the security environment (e.g., altering access control lists to permit attacks to enter a network).
- **(U)** Unauthorized interception and manipulation of network activity.
- **(U)** Disconnection of physical data links or connection of unauthorized data links.

(U) Server Rooms and Equipment Access

(U) OIG identified weaknesses in physical controls to the server room (b) (5) [redacted] at the IBWC's U. S. Section headquarters in El Paso, the IBWC field office in Fort Hancock, and at the San Diego wastewater treatment plant. Following OIG recommendations in FY 2011, IBWC had implemented a proximity card reader to limit access to authorized personnel to the second floor server room in El Paso. The San Diego and the Yuma field offices had installed a cipher lock that restricts access to only authorized personnel as well as bolting their server racks to the floor.

[74] **(U)** NIST SP 800-82, "Executive Summary," June 2011.

(U) OIG observed the following physical control deficiencies:

- **(U)** Third floor equipment room in El Paso and the Fort Hancock field office had not been restricted to authorized personnel.
- **(U)** All IBWC El Paso file server racks were not locked.
- **(U)** IBWC El Paso and the San Diego wastewater treatment plant server racks were not bolted to the floor.

(U) According to NIST SP 800-53, Revision 3,[75] "the organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible), issues authorization credentials, reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing, from the access list personnel no longer requiring access." An IBWC official stated that no formal physical and environmental protection plan existed. Without an effective physical protection plan, personnel may be unaware of risks that could compromise the confidentiality, integrity, and availability of data.

(U) Environmental Protection Weaknesses

(U) Environmental protection controls are designed to protect employee safety and IT assets from damage and destruction. OIG determined that some environmental protections in place at IBWC offices were insufficient to adequately protect personnel and property. Specifically, OIG found the following environmental protection weaknesses:

- **(U)** IBWC San Diego and Yuma field offices had not maintained fire suppression and detection devices sensitive to the water and humidity requirements of electrical equipment. For example, although the Yuma field office had installed a sprinkler system in its server room to combat fire hazards, the resulting water from the sprinkler system, if activated, could damage sensitive electronic equipment.
- **(U)** The IBWC San Diego field office did not have a way to shut down electricity or provide emergency lighting within the computer area in the event of an emergency, which could result in damage to equipment or injury to personnel.

(U) NIST SP 800-53, Revision 3,[76] states that "the organization protects power equipment and power cabling for the information system from damage and destruction." NIST SP 800-53, Revision 3, also states the following:

[75] **(U)** NIST SP 800-53, rev. 3, PE-2.

[76] **(U)** NIST SP 800-53, rev. 3, PE-9 "Power Equipment and Power Cabling," Aug. 2009 (last updated May 2010).

- **(U)** "The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.[77]

- **(U)** The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.[78]

- **(U)** The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.[79]

- **(U)** The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source."[80]

(U) An IBWC official stated that no formal physical and environmental protection plan existed. Without an effective environmental protection plan, personnel may be unaware of risks that could result in injuries to personnel and damage or destruction of IBWC IT assets.

(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.

~~(SBU)~~ **Management Response.** IBWC concurred with the recommendation, stating that the San Diego Field Office Area Operations Manager, "in coordination with the Veolia Superintendant," had implemented an accountability plan that "responds to necessary procedures and controls over proximity access cards and remote gate devices" and that the policy and procedures had been updated and are being finalized.

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented chain-of-custody procedures to control access to the proximity access cards and remote gate devices along the international border.

(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.

~~(SBU)~~ **Management Response.** IBWC concurred with the recommendation, stating that the current update to the existing SCADA System at the SBIWTP was being evaluated to

[77] **(U)** NIST SP 800-53, rev. 3, PE-10 "Emergency Shutoff," Aug. 2009 (last updated May 2010).
[78] **(U)** NIST SP 800-53, rev. 3, PE-11 "Emergency Power," Aug. 2009 (last updated May 2010).
[79] **(U)** NIST SP 800-53, rev. 3, PE-12 "Emergency Lighting," Aug. 2009 (last updated May 2010).
[80] **(U)** NIST SP 800-53, rev. 3, PE-13 "Fire Protection," Aug. 2009 (last updated May 2010).

ensure that the items specified in the recommendation were addressed, including the "physical access, deficiencies and requirement of auto-locking screens for PLC and HMI interfaces throughout the plant." IBWC stated that it anticipated having the new security features and updated systems in place by September 2013.

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has developed and implemented physical access controls to restrict access to the SCADA control centers, PLC, and file servers as required.

(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.

~~(SBU)~~ Management Response. IBWC concurred with the recommendation, stating that the current proposed update to the existing SCADA System at the SBIWTP was being evaluated to ensure that the items specified in the recommendation are addressed, including the physical access to servers at the SBWITP. IBWC further stated that a "half rack" had been installed at the Ft. Hancock office and that this rack restricted access to network components installed there. IBWC stated that it was finalizing work that would expand the IBWC LAN room, "providing more sufficient cooling, allow for growth and address the requirement of having all server racks bolted to the floor to prevent damage to equipment or harm to employees."

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has restricted access to file servers at its San Diego, CA, wastewater treatment plant and the field offices in Fort Hancock and its headquarters in El Paso and ensures that the servers are attached to the floor to prevent damage to equipment or harm to employees as required.

(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) Management Response. IBWC concurred with the recommendation, stating that an assessment of all IBWC server rooms would be conducted in early 2013 "to determine the most cost-effective protective measures to prevent fire and damage to file servers."

(U) OIG Reply. OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approves documentation showing that IBWC has determined the most cost-effective protective measures to prevent fire and damage to file servers as required.

(U) List of Recommendations

(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) 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) 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) 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.

~~(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) 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) 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) 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) 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) 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) 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) 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) 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) 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) 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.

~~(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) 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) 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) 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.

~~(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.

(b) (5) [redacted]

~~(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) 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) 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) 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) 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) 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) 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) 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) 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) 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) Appendix A

(U) Objective, Scope, and Methodology

(U) The objective of this audit was to determine the effectiveness of U.S. Section, International Boundary and Water Commission (IBWC), information security program and practices.

(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).[1] DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

(U) To fulfill its responsibilities required by FISMA, the Office of Inspector General (OIG), Office of Audits, conducted fieldwork at the El Paso, TX, headquarters; the San Diego, CA, Yuma, AZ, and Fort Hancock, TX, field offices; and the continuity of operations site at Las Cruces, NM, to evaluate the IBWC information technology (IT) security program and practices and to determine the effectiveness of the program for FY 2012. OIG interviewed IBWC senior management, employees, and contractors and evaluated managerial effectiveness and operational controls. OIG observed daily operations and obtained evidence to support OIG conclusions and recommendations and collected written documents to augment observations and interviews.

(U) OIG conducted its audit from April 2012 through July 2012 and its fieldwork from April 2012 through June 2012. In addition, OIG performed the audit in accordance with generally accepted government auditing standards (GAGAS) and in accordance with FISMA, OMB, and National Institute of Standards and Technology Special Publication guidance. 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 findings with and proposed recommendations with to IBWC officials on August 23, 2012. Additionally, an interim discussion was conducted with IBWC Information Management Division personnel.

[1] **(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 better 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 and Data Reliability

(U) The audit team used computer-generated data from IBWC during this audit. To assess the reliability of computer-processed data, OIG reviewed electronic documentation related to IT personnel investigation requirements and performed tracing of data to source documentation. Specifically, OIG obtained and reviewed personnel security policies with members of the Information Management Division (IMD) to identify the IBWC staff responsible for IT security functions requiring background investigations. OIG determined that the data were sufficiently reliable to support the conclusions and recommendations of this report.

(U) Appendix B

(U) Office of Inspector General
FY 2011 Federal Information Security Management Act Report
Statuses of Recommendations

(U) The FY 2011 Federal Information Security Management Act (FISMA) evaluation was conducted by the Department of State, Office of Inspector General (OIG), Office of Audits, and contained 21 recommendations.[1] 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 2011 FISMA report. Below is the current status of each recommendation:

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendations 1 and 2 (Finding A) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 3 (Finding B) in the FY 2012 report.*

(U) Recommendation 3. OIG recommends that the Chief Information Officer:

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

[1] **(U)** *Evaluation of the United States Section, International Boundary and Water Commission, Information Security Program* (AUD/IT-12-16, November 2011).

- **~~(SBU)~~** Perform annual security assessments of a subset of a system's security controls, as required by NIST SP 800-37, Revision 1.

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendations 4 - 7 (Finding B) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 8 (Finding C) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 9 (Finding C) in the FY 2012 report.*

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

(U) *Status: Closed January 2012*. IBWC's Information Management Division (IMD) conducted five information technology (IT) security training classes immediately after the OIG visit in August 2011, resulting in 235 of 272 employees completing annual IT security training. IBWC acquired a cloud based training system that will allow for a much more efficient method to provide IT security training to IBWC personnel.

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 13 (Finding E) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 14 (Finding F) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 15 (Finding G) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 20 (Finding I) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 22 (Finding J) in the FY 2012 report.*

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

(U) *Status: Closed April 2012*. IBWC acquired the needed client to allow for the full offsite backup of all field offices.

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 23 (Finding K) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 24 (Finding K) in the FY 2012 report.*

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

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 25 (Finding L) in the FY 2012 report.*

(U) Recommendation 16. OIG recommends that International Boundary and Water Commission (IBWC) devote attention and resources to ensure that all IBWC employees and contractors undergo background investigations and formal clearance adjudication, as required by Homeland Security Presidential Directive 12.

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 26 and 27 (Finding M) in the FY 2012 report.*

~~(SBU)~~ Recommendation 17. OIG recommends that the International Boundary and Water Commission develop and implement chain-of-custody procedures to control access to and use of remote gate devices along the international border.

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 28 (Finding N) in the FY 2012 report.*

~~(SBU)~~ Recommendation 18. OIG recommends that the International Boundary and Water Commission (IBWC) collaborate with the Department of Homeland Security to ensure that IBWC-sponsored entry into the United States is appropriately inspected by U.S. Customs and Border Protection.

(U) *Status: Closed April 2012.* IBWC entered into an agreement with the U.S. Customs and Border Protection, a component of the Department of Homeland Security, detailing the inspection actions by U.S. Customs and Border Protection of IBWC-sponsored entry.

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

(U) *Status: Closed April 2012*. IBWC reviewed the access to server room and prepared a current list of Information Management Division staff that has been granted access.

(U) Recommendation 20. OIG recommends that the International Boundary and Water Commission restrict access to file servers at its San Diego, CA waste treatment plant, the field offices in San Diego and Yuma, AZ, 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 2011 FISMA report. It has become Recommendation 30 (Finding N) in the FY 2012 report.*

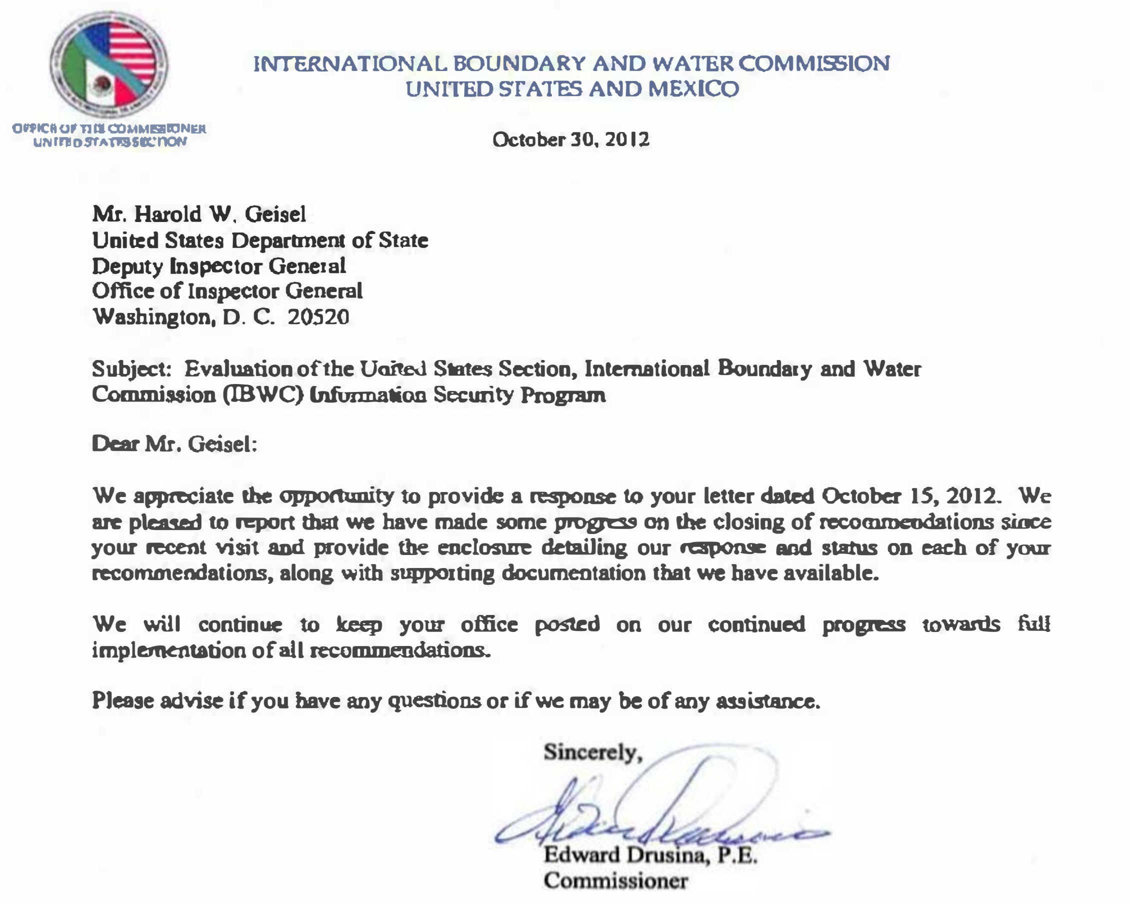
(b) (5)

[redacted]

(U) *Status: Closed from the FY 2011 FISMA report. It has become Recommendation 31 (Finding N) in the FY 2012 report.*

(U) Appendix C

(U) International Boundary and Water Commission Response



OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

October 30, 2012

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

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

Dear Mr. Geisel:

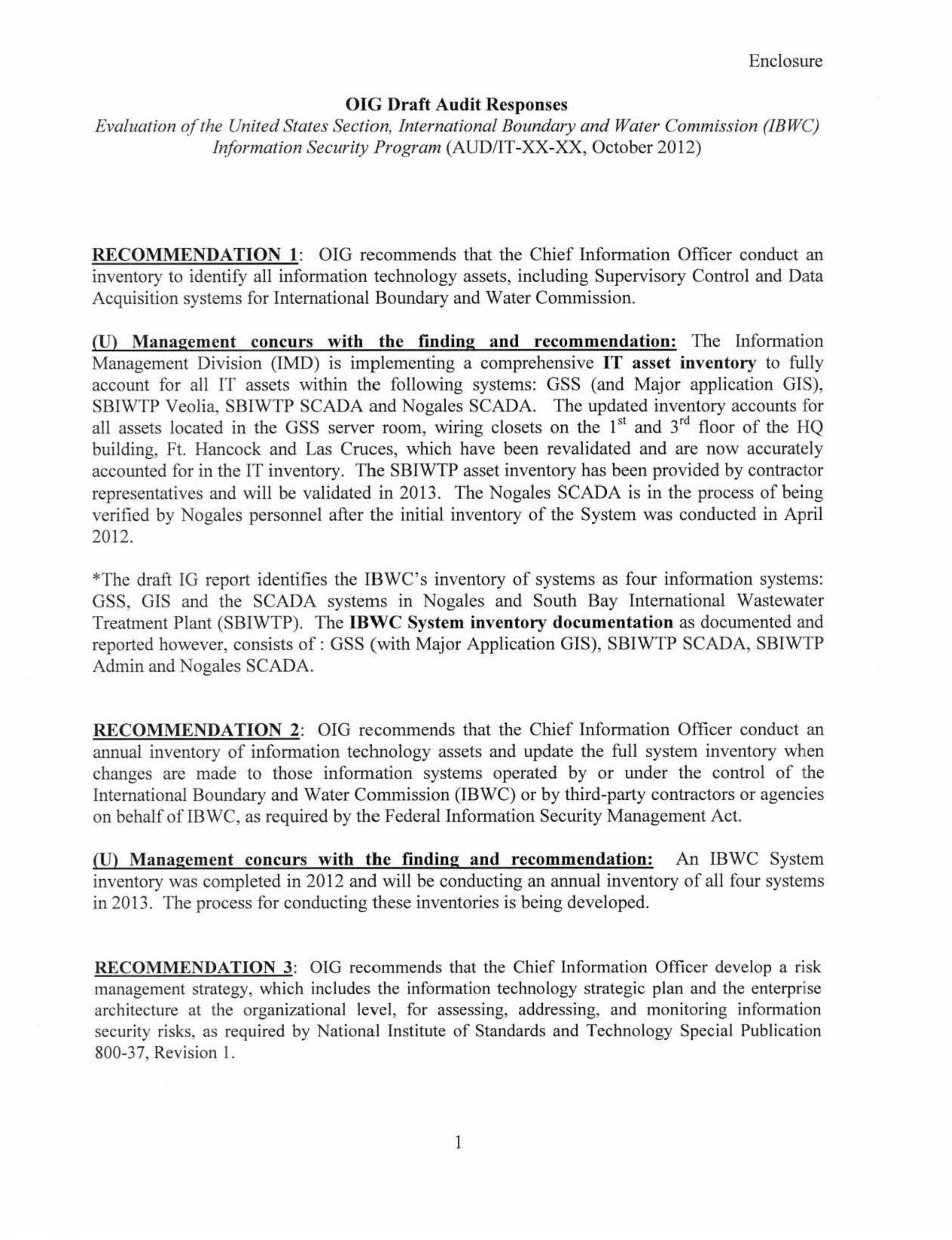
We appreciate the opportunity to provide a response to your letter dated October 15, 2012. We are pleased to report that we have made some progress on the closing of recommendations since your recent visit and provide the enclosure detailing our response and status on each of your recommendations, along with supporting documentation that we have available.

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



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

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) Management concurs with the finding and recommendation: The Information Management Division (IMD) is implementing a comprehensive **IT asset inventory** to fully account for all IT assets within the following systems: GSS (and Major application GIS), SBIWTP Veolia, SBIWTP SCADA and Nogales SCADA. The updated inventory accounts for all assets located in the GSS server room, wiring closets on the 1st and 3rd floor of the HQ building, Ft. Hancock and Las Cruces, which have been revalidated and are now accurately accounted for in the IT inventory. The SBIWTP asset inventory has been provided by contractor representatives and will be validated in 2013. The Nogales SCADA is in the process of being verified by Nogales personnel after the initial inventory of the System was conducted in April 2012.

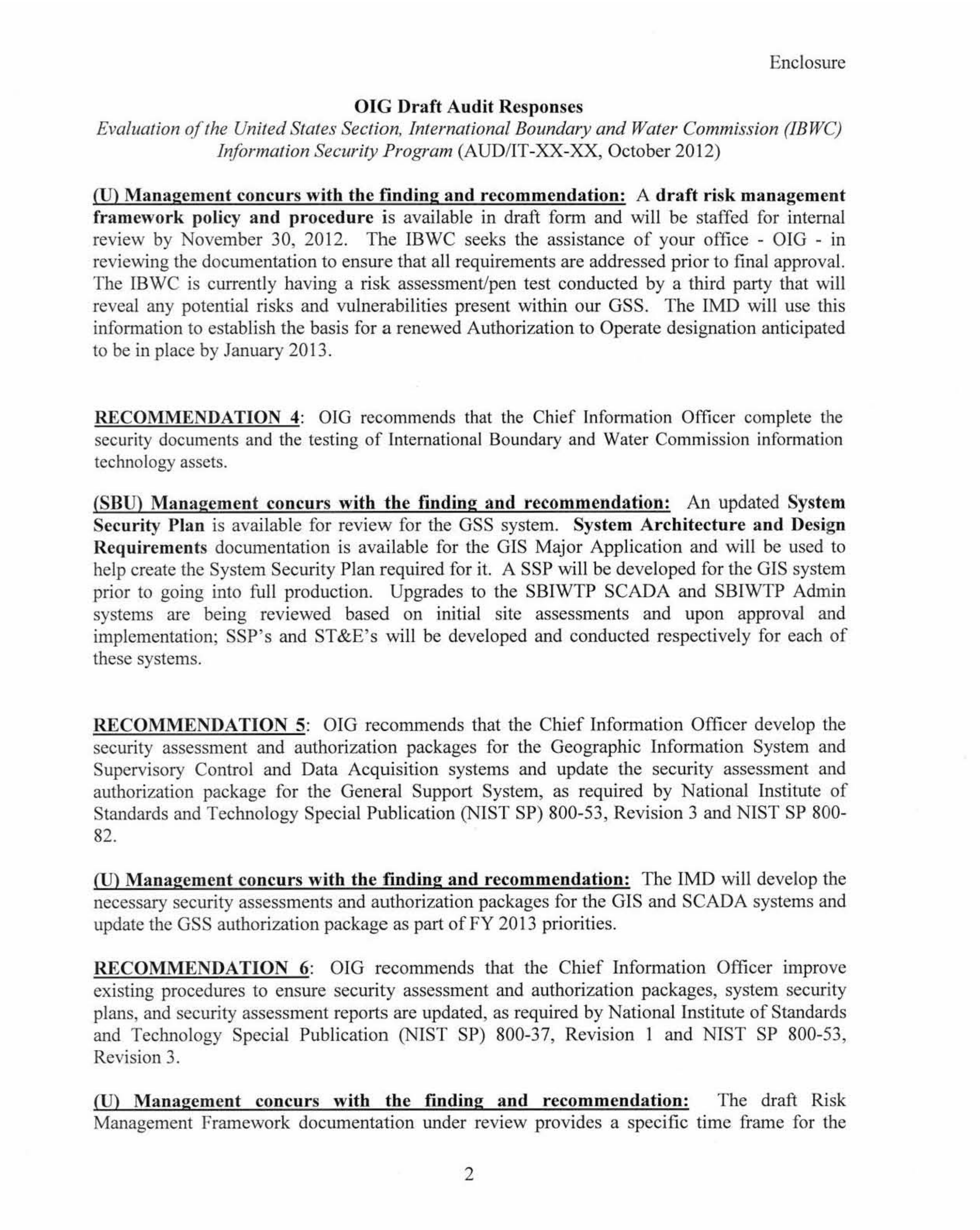
*The draft IG report identifies the IBWC's inventory of systems as four information systems: GSS, GIS and the SCADA systems in Nogales and South Bay International Wastewater Treatment Plant (SBIWTP). The **IBWC System inventory documentation** as documented and reported however, consists of : GSS (with Major Application GIS), SBIWTP SCADA, SBIWTP Admin and Nogales SCADA.

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) Management concurs with the finding and recommendation: An IBWC System inventory was completed in 2012 and will be conducting an annual inventory of all four systems in 2013. The process for conducting these inventories is being developed.

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.

1



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

(U) Management concurs with the finding and recommendation: A **draft risk management framework policy and procedure** is available in draft form and will be staffed for internal review by November 30, 2012. The IBWC seeks the assistance of your office - OIG - in reviewing the documentation to ensure that all requirements are addressed prior to final approval. The IBWC is currently having a risk assessment/pen test conducted by a third party that will reveal any potential risks and vulnerabilities present within our GSS. The IMD will use this information to establish the basis for a renewed Authorization to Operate designation anticipated to be in place by January 2013.

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.

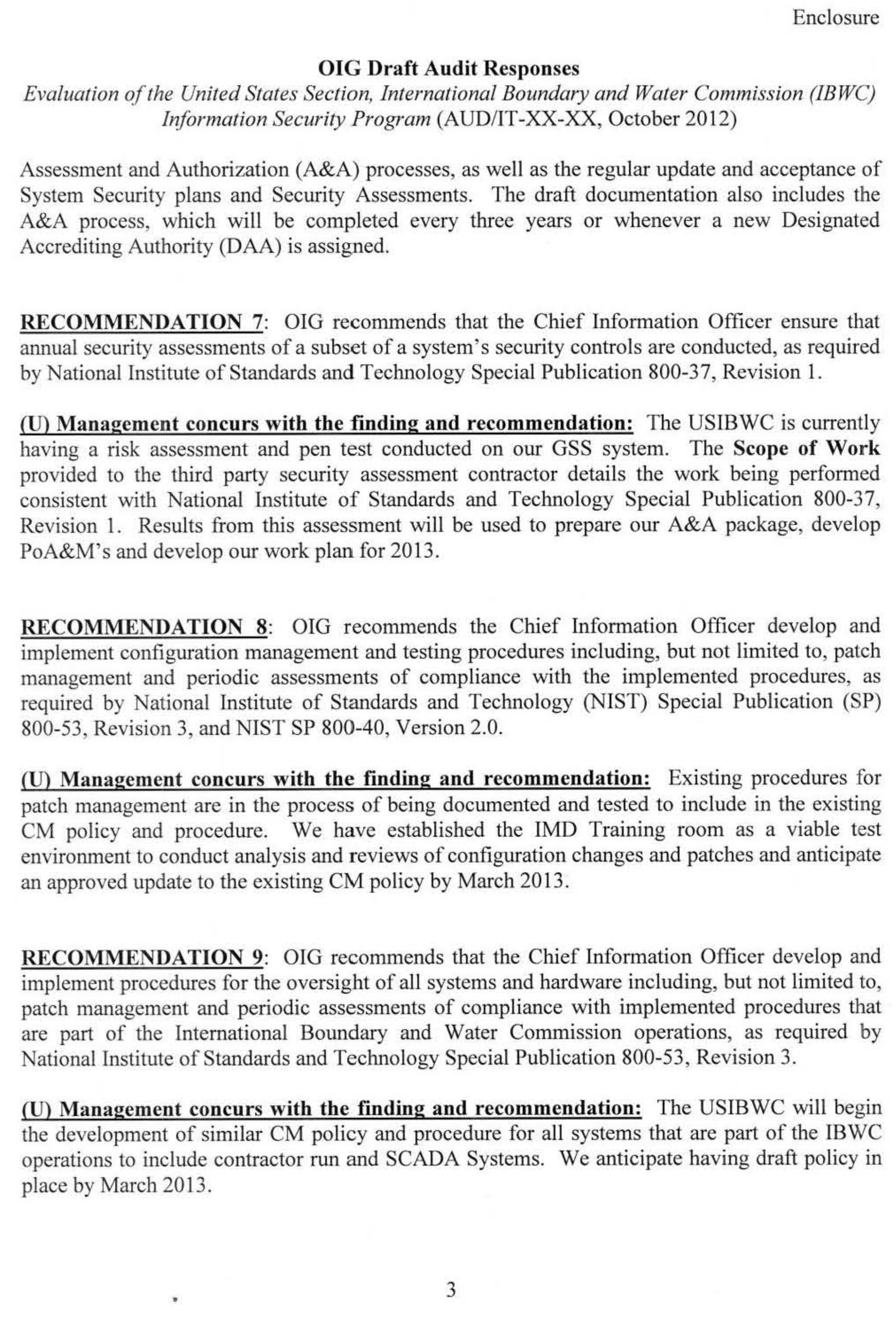
(SBU) Management concurs with the finding and recommendation: An updated **System Security Plan** is available for review for the GSS system. **System Architecture and Design Requirements** documentation is available for the GIS Major Application and will be used to help create the System Security Plan required for it. A SSP will be developed for the GIS system prior to going into full production. Upgrades to the SBIWTP SCADA and SBIWTP Admin systems are being reviewed based on initial site assessments and upon approval and implementation; SSP's and ST&E's will be developed and conducted respectively for each of these systems.

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) Management concurs with the finding and recommendation: The IMD will develop the necessary security assessments and authorization packages for the GIS and SCADA systems and update the GSS authorization package as part of FY 2013 priorities.

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) Management concurs with the finding and recommendation: The draft Risk Management Framework documentation under review provides a specific time frame for the



Enclosure

OIG Draft Audit Responses
Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

Assessment and Authorization (A&A) processes, as well as the regular update and acceptance of System Security plans and Security Assessments. The draft documentation also includes the A&A process, which will be completed every three years or whenever a new Designated Accrediting Authority (DAA) is assigned.

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.

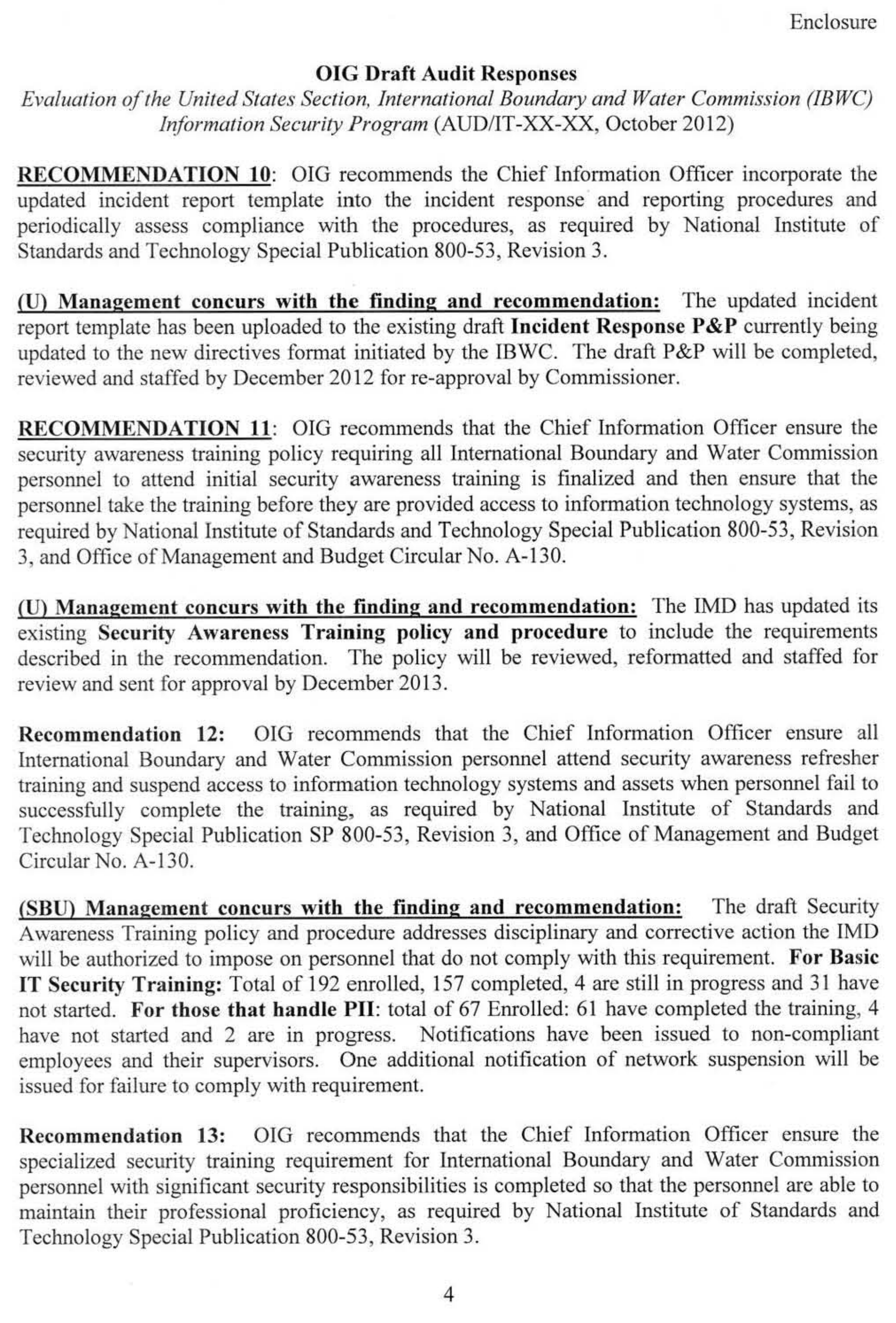
(U) Management concurs with the finding and recommendation: The USIBWC is currently having a risk assessment and pen test conducted on our GSS system. The **Scope of Work** provided to the third party security assessment contractor details the work being performed consistent with National Institute of Standards and Technology Special Publication 800-37, Revision 1. Results from this assessment will be used to prepare our A&A package, develop PoA&M's and develop our work plan for 2013.

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) Management concurs with the finding and recommendation: Existing procedures for patch management are in the process of being documented and tested to include in the existing CM policy and procedure. We have established the IMD Training room as a viable test environment to conduct analysis and reviews of configuration changes and patches and anticipate an approved update to the existing CM policy by March 2013.

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) Management concurs with the finding and recommendation: The USIBWC will begin the development of similar CM policy and procedure for all systems that are part of the IBWC operations to include contractor run and SCADA Systems. We anticipate having draft policy in place by March 2013.



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

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) Management concurs with the finding and recommendation: The updated incident report template has been uploaded to the existing draft **Incident Response P&P** currently being updated to the new directives format initiated by the IBWC. The draft P&P will be completed, reviewed and staffed by December 2012 for re-approval by Commissioner.

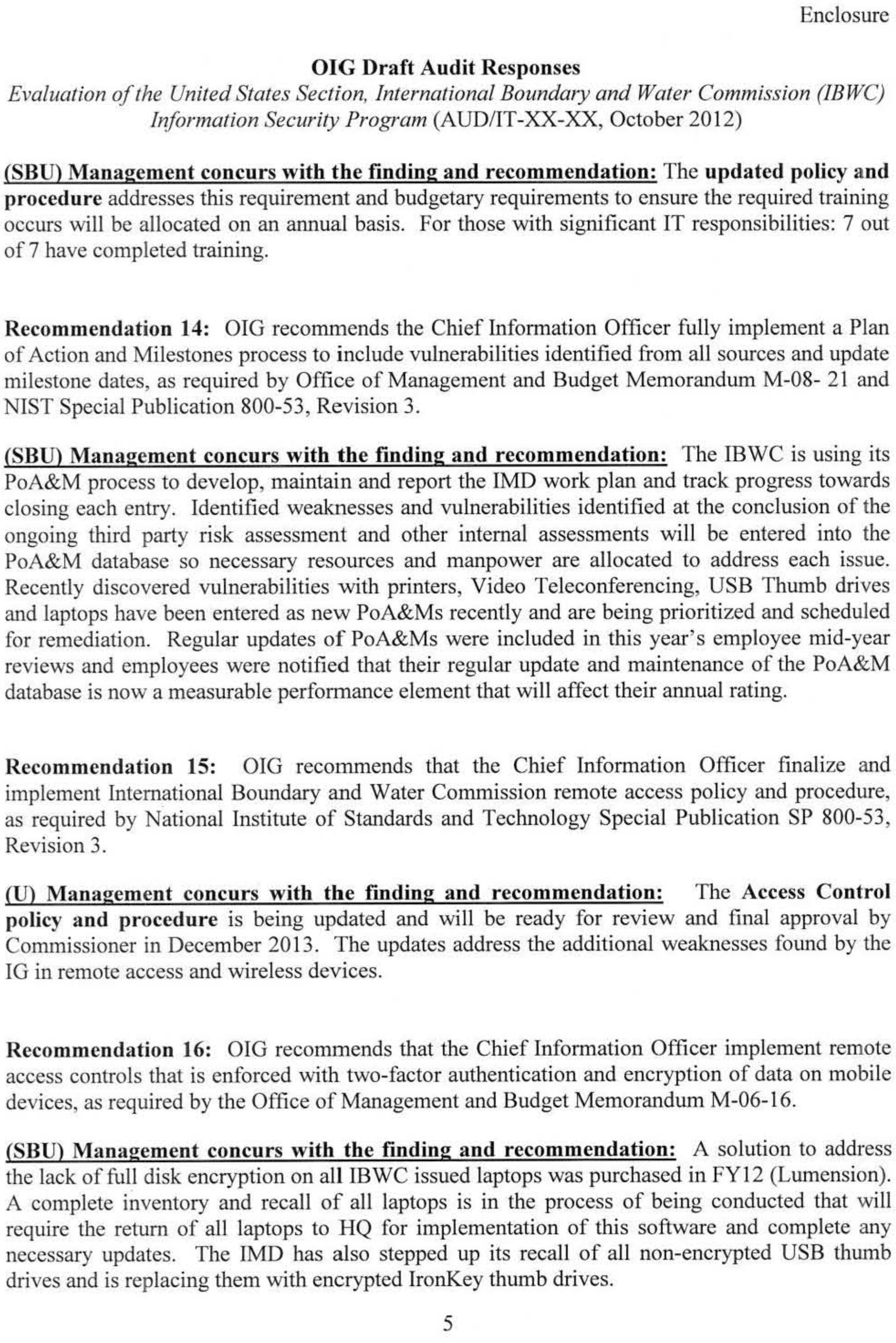
RECOMMENDATION 11: OIG recommends that the Chief Information Officer ensure the security awareness training policy requiring all International Boundary and Water Commission personnel to attend initial security awareness training is finalized and then ensure that the personnel take the training before 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) Management concurs with the finding and recommendation: The IMD has updated its existing **Security Awareness Training policy and procedure** to include the requirements described in the recommendation. The policy will be reviewed, reformatted and staffed for review and sent for approval by December 2013.

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.

(SBU) Management concurs with the finding and recommendation: The draft Security Awareness Training policy and procedure addresses disciplinary and corrective action the IMD will be authorized to impose on personnel that do not comply with this requirement. **For Basic IT Security Training:** Total of 192 enrolled, 157 completed, 4 are still in progress and 31 have not started. **For those that handle PII**: total of 67 Enrolled: 61 have completed the training, 4 have not started and 2 are in progress. Notifications have been issued to non-compliant employees and their supervisors. One additional notification of network suspension will be issued for failure to comply with requirement.

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.



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

(SBU) Management concurs with the finding and recommendation: The **updated policy and procedure** addresses this requirement and budgetary requirements to ensure the required training occurs will be allocated on an annual basis. For those with significant IT responsibilities: 7 out of 7 have completed training.

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.

(SBU) Management concurs with the finding and recommendation: The IBWC is using its PoA&M process to develop, maintain and report the IMD work plan and track progress towards closing each entry. Identified weaknesses and vulnerabilities identified at the conclusion of the ongoing third party risk assessment and other internal assessments will be entered into the PoA&M database so necessary resources and manpower are allocated to address each issue. Recently discovered vulnerabilities with printers, Video Teleconferencing, USB Thumb drives and laptops have been entered as new PoA&Ms recently and are being prioritized and scheduled for remediation. Regular updates of PoA&Ms were included in this year's employee mid-year reviews and employees were notified that their regular update and maintenance of the PoA&M database is now a measurable performance element that will affect their annual rating.

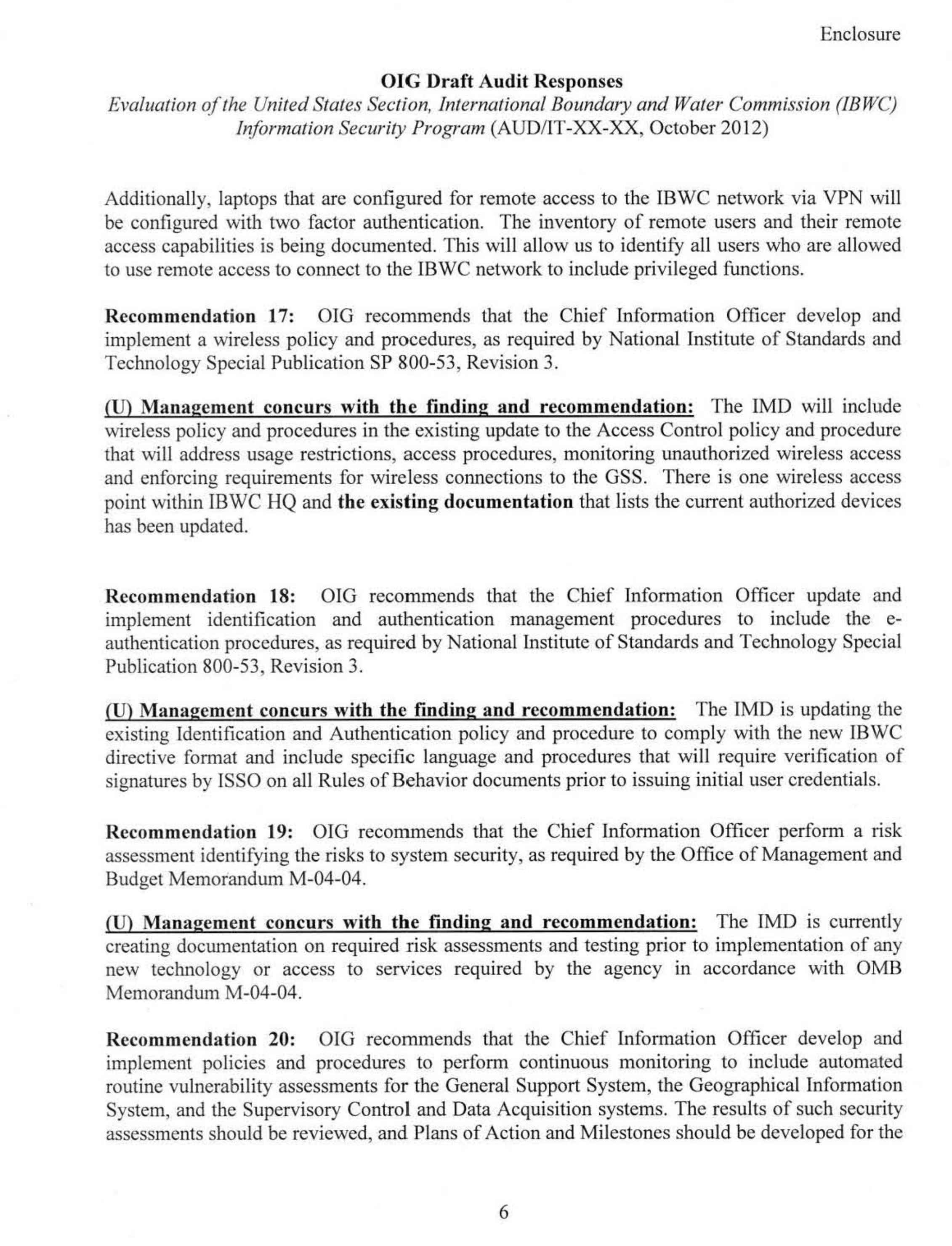
Recommendation 15: OIG recommends that the Chief Information Officer finalize and implement International Boundary and Water Commission remote access policy and procedure, as required by National Institute of Standards and Technology Special Publication SP 800-53, Revision 3.

(U) Management concurs with the finding and recommendation: The **Access Control policy and procedure** is being updated and will be ready for review and final approval by Commissioner in December 2013. The updates address the additional weaknesses found by the IG in remote access and wireless devices.

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.

(SBU) Management concurs with the finding and recommendation: A solution to address the lack of full disk encryption on all IBWC issued laptops was purchased in FY12 (Lumension). A complete inventory and recall of all laptops is in the process of being conducted that will require the return of all laptops to HQ for implementation of this software and complete any necessary updates. The IMD has also stepped up its recall of all non-encrypted USB thumb drives and is replacing them with encrypted IronKey thumb drives.

5



Enclosure

OIG Draft Audit Responses
Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

Additionally, laptops that are configured for remote access to the IBWC network via VPN will be configured with two factor authentication. The inventory of remote users and their remote access capabilities is being documented. This will allow us to identify all users who are allowed to use remote access to connect to the IBWC network to include privileged functions.

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) Management concurs with the finding and recommendation: The IMD will include wireless policy and procedures in the existing update to the Access Control policy and procedure that will address usage restrictions, access procedures, monitoring unauthorized wireless access and enforcing requirements for wireless connections to the GSS. There is one wireless access point within IBWC HQ and **the existing documentation** that lists the current authorized devices has been updated.

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) Management concurs with the finding and recommendation: The IMD is updating the existing Identification and Authentication policy and procedure to comply with the new IBWC directive format and include specific language and procedures that will require verification of signatures by ISSO on all Rules of Behavior documents prior to issuing initial user credentials.

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) Management concurs with the finding and recommendation: The IMD is currently creating documentation on required risk assessments and testing prior to implementation of any new technology or access to services required by the agency in accordance with OMB Memorandum M-04-04.

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

Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

improvement of the security controls of major systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

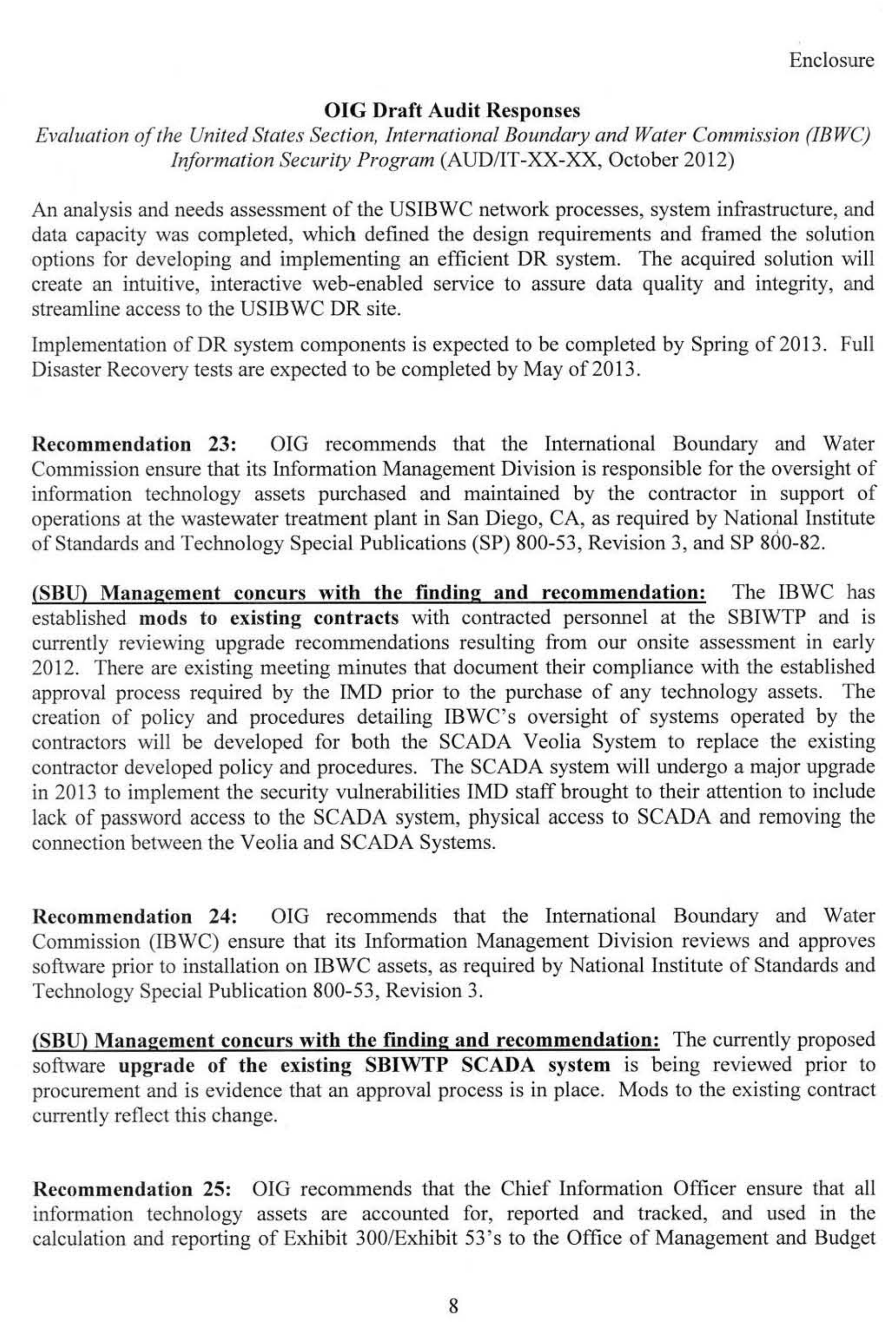
(SBU) Management concurs with the finding and recommendation: The IMD is in the process of developing policies and procedures to assist in the full implementation of an effective continuous monitoring program for its IT Systems. The IMD has received approval for a permanent, part time employee whose main responsibility will be many of the tasks required to maintain a continuous monitoring program. Tasks identified include but are not limited to log monitoring, vulnerability scanning, detection of unauthorized devices and acting on results of vulnerability scans in a timely manner. Additional duties will also include ensuring PoA&M's include identified vulnerabilities based on monitoring results, maintaining change control management documentation and conducting Security Test and Evaluations necessary for all IBWC Systems (to include SCADA systems) to ensure regular evaluation of security controls.

(b) (5) [redacted]

(SBU) Management concurs with the finding and recommendation: The IMD is updating existing **COOP documentation** to reflect significant changes to the environment and to enable testing of the agency's disaster recovery solution. The USIBWC is also developing a Business Impact Assessment to help identify and prioritize critical IT systems and components. A "warm" disaster recover site will be implemented and existing backup infrastructure will be used as part of the disaster recovery plan and enable the access of backup data directly to IBWC employees. Testing of the disaster recovery plan with recently acquired hardware and software is scheduled for May 2013.

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.

(SBU) Management concurs with the finding and recommendation: In September the IMD awarded a contract to assist with the implementation of a VMWare and Cisco Virtualization solution with Citrix for secure web access for a Disaster Recovery (DR) system at the Las Cruces COOP site. This solution is to serve as a centralized source of backup hardware/software and data to be shared across all USIBWC divisions and will enable accessed to authorized USIBWC personnel during a disaster recovery.



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

An analysis and needs assessment of the USIBWC network processes, system infrastructure, and data capacity was completed, which defined the design requirements and framed the solution options for developing and implementing an efficient DR system. The acquired solution will create an intuitive, interactive web-enabled service to assure data quality and integrity, and streamline access to the USIBWC DR site.

Implementation of DR system components is expected to be completed by Spring of 2013. Full Disaster Recovery tests are expected to be completed by May of 2013.

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.

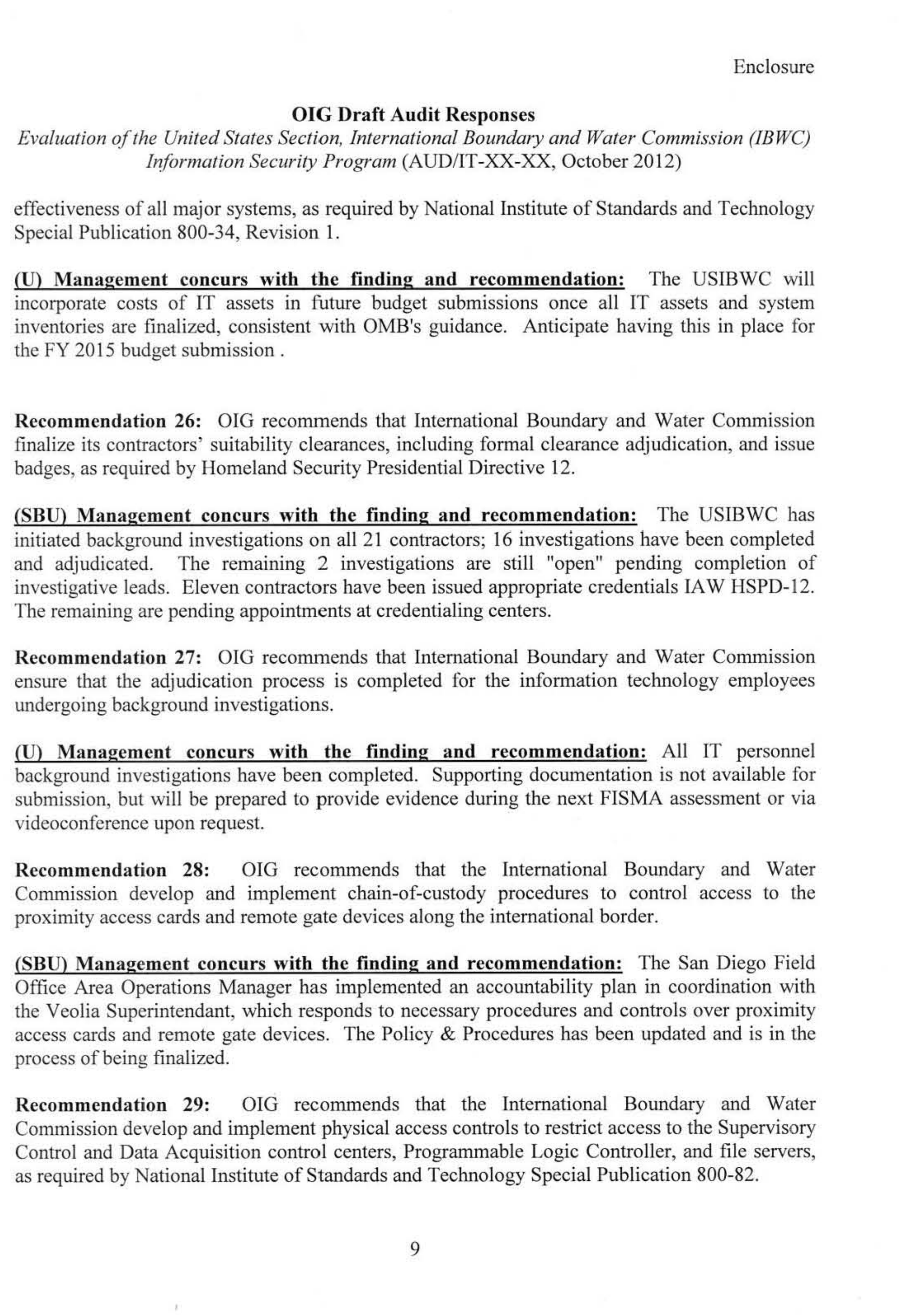
(SBU) Management concurs with the finding and recommendation: The IBWC has established **mods to existing contracts** with contracted personnel at the SBIWTP and is currently reviewing upgrade recommendations resulting from our onsite assessment in early 2012. There are existing meeting minutes that document their compliance with the established approval process required by the IMD prior to the purchase of any technology assets. The creation of policy and procedures detailing IBWC's oversight of systems operated by the contractors will be developed for both the SCADA Veolia System to replace the existing contractor developed policy and procedures. The SCADA system will undergo a major upgrade in 2013 to implement the security vulnerabilities IMD staff brought to their attention to include lack of password access to the SCADA system, physical access to SCADA and removing the connection between the Veolia and SCADA Systems.

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.

(SBU) Management concurs with the finding and recommendation: The currently proposed software **upgrade of the existing SBIWTP SCADA system** is being reviewed prior to procurement and is evidence that an approval process is in place. Mods to the existing contract currently reflect this change.

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

8



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

effectiveness of all major systems, as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) Management concurs with the finding and recommendation: The USIBWC will incorporate costs of IT assets in future budget submissions once all IT assets and system inventories are finalized, consistent with OMB's guidance. Anticipate having this in place for the FY 2015 budget submission .

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.

(SBU) Management concurs with the finding and recommendation: The USIBWC has initiated background investigations on all 21 contractors; 16 investigations have been completed and adjudicated. The remaining 2 investigations are still "open" pending completion of investigative leads. Eleven contractors have been issued appropriate credentials IAW HSPD-12. The remaining are pending appointments at credentialing centers.

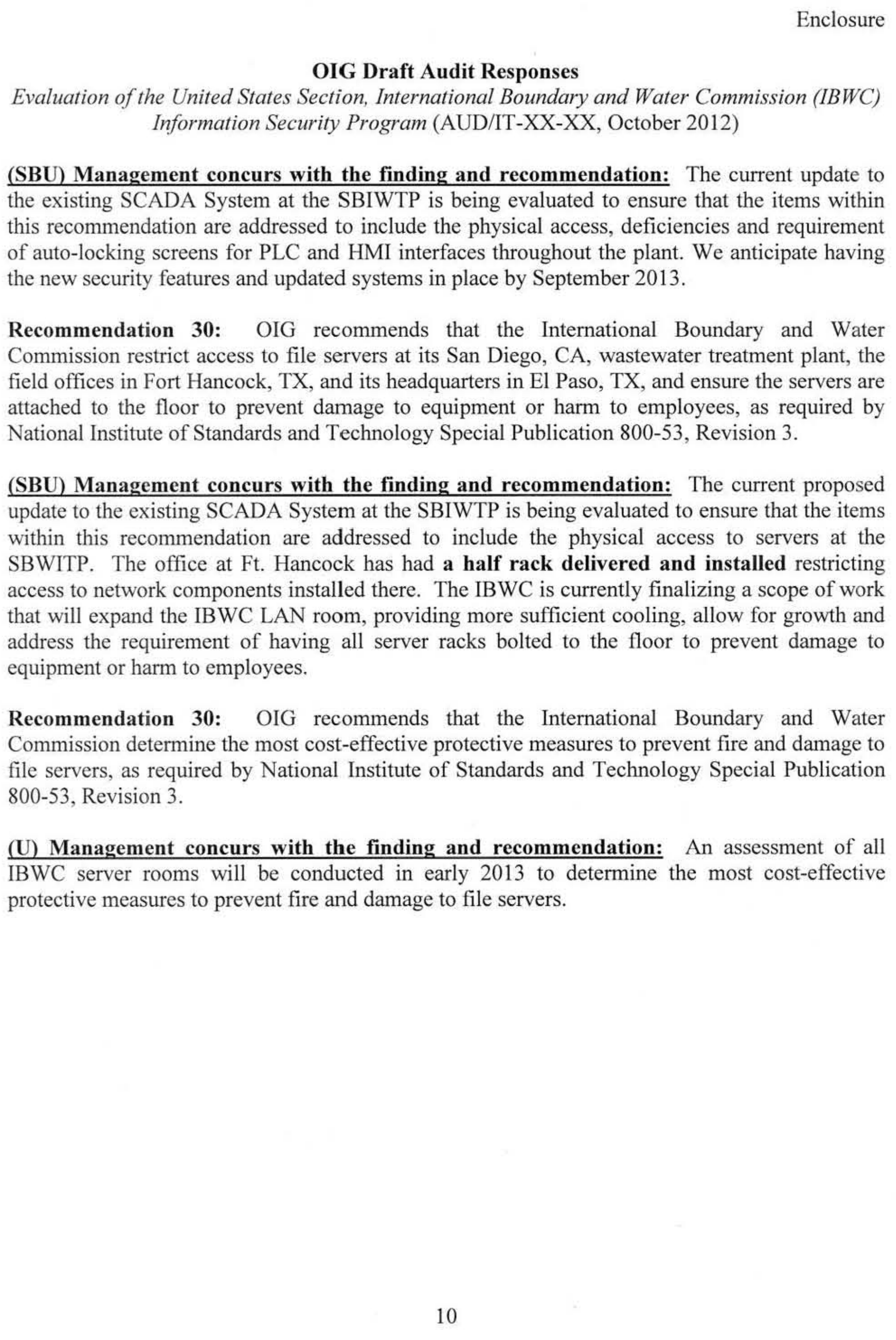
Recommendation 27: OIG recommends that International Boundary and Water Commission ensure that the adjudication process is completed for the information technology employees undergoing background investigations.

(U) Management concurs with the finding and recommendation: All IT personnel background investigations have been completed. Supporting documentation is not available for submission, but will be prepared to provide evidence during the next FISMA assessment or via videoconference upon request.

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.

(SBU) Management concurs with the finding and recommendation: The San Diego Field Office Area Operations Manager has implemented an accountability plan in coordination with the Veolia Superintendant, which responds to necessary procedures and controls over proximity access cards and remote gate devices. The Policy & Procedures has been updated and is in the process of being finalized.

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.



Enclosure

OIG Draft Audit Responses

Evaluation of the United States Section, International Boundary and Water Commission (IBWC) Information Security Program (AUD/IT-XX-XX, October 2012)

(SBU) Management concurs with the finding and recommendation: The current update to the existing SCADA System at the SBIWTP is being evaluated to ensure that the items within this recommendation are addressed to include the physical access, deficiencies and requirement of auto-locking screens for PLC and HMI interfaces throughout the plant. We anticipate having the new security features and updated systems in place by September 2013.

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.

(SBU) Management concurs with the finding and recommendation: The current proposed update to the existing SCADA System at the SBIWTP is being evaluated to ensure that the items within this recommendation are addressed to include the physical access to servers at the SBWITP. The office at Ft. Hancock has had **a half rack delivered and installed** restricting access to network components installed there. The IBWC is currently finalizing a scope of work that will expand the IBWC LAN room, providing more sufficient cooling, allow for growth and address the requirement of having all server racks bolted to the floor to prevent damage to equipment or harm to employees.

Recommendation 30: 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) Management concurs with the finding and recommendation: An assessment of all IBWC server rooms will be conducted in early 2013 to determine the most cost-effective protective measures to prevent fire and damage to file servers.

(U) Major Contributors to This Report

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

(U) Mr. Steve Matthews, Audit Manager
Information Technology Division,
Office of Audits

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

(U) Ms. Jamie Horvath, Senior Auditor
Information Technology Division,
Office of Audits