OIG HIGHLIGHTS

View Report AUD-IT-16-07.

November 2015
OFFICE OF AUDITS
Information Technology Division

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

(U) What OIG Audited

(U) The Office of Inspector General (OIG) conducted this audit to assess the effectiveness of the International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC), information security program in accordance with the Federal Information Security Management Act (FISMA). Specifically, OIG assessed USIBWC's information security program and related practices for risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring, contingency planning, oversight of contractor systems, access controls, personnel security, and physical and environmental protection.

(U) What OIG Recommends

~~(SBU)~~ OIG made three repeat recommendations, with revision to address progress made relating to the [Redacted] (b) (5) at its [Redacted] (b) (5) International Wastewater Treatment Plant [Redacted] (b) (5) and [Redacted] (b) (5) International Wastewater Treatment Plant [Redacted] (b) (5)

(U) Based on USIBWC's responses to the draft report, OIG considers all recommendations resolved, pending further action.

(U) What OIG Found

~~(SBU)~~ During FY 2015, USIBWC implemented an effective information security program for its General Support System, but additional actions are needed to fully secure its [Redacted] (b) (5) Specifically, OIG found that USIBWC executed a contract to obtain expertise to design and implement an upgrade strategy for the [Redacted] (b) (5) at its [Redacted] (b) (5) However, as of August 2015, USIBWC has not fully completed implementation of the [Redacted] (b) (5) upgrade design, including [Redacted] (b) (5) improvements. According to USIBWC officials, implementation has not been completed for [Redacted] (b) (5) systems due to the time required to award a contract and acquire the technical resources to design a [Redacted] (b) (5) upgrade strategy. Until an upgrade strategy and [Redacted] (b) (5) improvements are implemented, the confidentiality, integrity, and availability of the [Redacted] (b) (5) will remain at increased risk.

~~(SBU)~~ OIG also found that the upgrade strategy includes steps to implement an [Redacted] (b) (5) However, the [Redacted] (b) (5) was not fully implemented at the time of our audit fieldwork because USIBWC had not fully obtained the technical resources needed to implement the strategy. Without full implementation of the [Redacted] (b) (5), there is increased risk that threats and vulnerabilities to USIBWC's [Redacted] could go undetected, which may lead to potential damage or disruption to the services provided by the [Redacted] (b) (5)

~~(SBU)~~ Finally, the current [Redacted] (b) (5) operation and maintenance contract does not contain provisions that ensure the contractor-operated [Redacted] (b) (5) that are compliant with FISMA. USIBWC executed a new contract in September 2015 that intends to bring its [Redacted] (b) (5) system closer to compliance with FISMA. USIBWC is also developing an upgrade strategy for its [Redacted] (b) (5) [Redacted] (b) (5) However, until the upgrade strategy is fully implemented, the [Redacted] (b) (5) will remain non-compliant with FISMA, potentially rendering it susceptible to outside attacks and insider threats.

OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-16-07 | Office of Audits | November 2015

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

INFORMATION TECHNOLOGY DIVISION

(U) CONTENTS

(U) OBJECTIVE

(U) The Office of Inspector General (OIG) conducted this audit to assess the effectiveness of the International Boundary and Water Commission, United States and Mexico, U.S. Section's (USIBWC) information security program in FY 2015. Specifically, OIG assessed USIBWC's information security program and related practices for risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring, contingency planning, oversight of contractor systems, access controls, personnel security, and physical and environmental protection. See Appendix A for the scope and methodology for this audit.

(U) BACKGROUND

(U) IBWC is a binational commission, created by the Convention of 1889.[1] IBWC has responsibility for applying the boundary and water treaties between the United States and Mexico. IBWC is composed of the United States Section and the Mexican Section. Each Section is administered independently of the other, and is headed by an Engineer Commissioner, appointed by his/her respective President. USIBWC is a Federal government agency that is headquartered in El Paso, Texas. USIBWC operates under the foreign policy guidance of the U.S. Department of State. The Mexican Section is headquartered in Ciudad Juarez, Chihuahua, Mexico and is under the administrative supervision of the Mexican Ministry of Foreign Affairs. The joint mission of the U.S. Section and the Mexican Section is to:

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

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

(U) USIBWC owns the [Redacted] (b) (5) which is responsible for meeting the [Redacted] (b) (5) USIBWC also maintains and operates the [Redacted] (b) (5) in accordance with the [Redacted] (b) (5) requirements mandated by the [Redacted] (b) (5) A photograph of the [Redacted] (b) (5) facility is presented in Figure 1.

[Redacted] (b) (5)

(U) Each [Redacted] (b) (5) has a [Redacted] (b) (5) system. The USIBWC systems are used to control dispersed assets through centralized data acquisition. Based on information received from remote stations, automated or operator-driven supervisory commands are controlled by remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

(U) Federal Information Security Management Act

(U) The Federal Information Security Management Act (FISMA) was enacted into law as Title III, Public Law No. 107-347, on December 17, 2002, and amended by the Federal Information Security Modernization Act of 2014, Public Law No. 113-283. Key requirements of FISMA are:

[2] (U) [Redacted] (b) (5) .

- (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 to test the effectiveness of information security policies, procedures, standards, and guidelines.

(U) The importance of information security to the economic and national security interests of the United States is underscored in FISMA. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over information technology that supports Federal agency information security programs.

(U) FISMA Reporting Areas

(U) There are 10 FISMA reportable areas:

1. (U) Configuration Management – intended to make assets harder to exploit through better configuration.

2. (U) Continuous Monitoring – intended to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management.

3. (U) Identity and Access Management – intended to make sure that access rights are only given to the intended individuals and/or processes.

4. (U) Incident Response and Reporting – intended to determine the kinds of attacks that have been successful and allows the organization to make a risk based decision about where it is most cost effective to focus its security resources.

5. (U) Risk Management – focuses on how the organization is evaluating risk and prioritizing security issues.

6. (U) Security Training – designed to train users and those with access to other pertinent information and media deterrents for cyberattacks, such as phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.

7. (U) Plan of Action & Milestones – considered an essential part of the risk management process to track problems and to decide which issues to address and to show efforts to address corrective action with a standard and centralized approach.

8. **(U)** Remote Access Management – intended to help deter, detect, and defend against unauthorized network connections/access to internal and external networks.

9. **(U)** Contingency Planning – its primary purpose is to give attention to rare events that have the potential for significant consequences and promoting first priority risk.

10. **(U)** Contractor Systems – intended to ensure that contractor systems are being managed to ensure that they have sufficient security.

(U) FISMA assigns specific responsibilities to the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS)[3] and other Federal agencies for the purpose of strengthening information system security throughout the Federal Government. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS. DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA. See Appendix B for the status of recommendations from the FY 2014 OIG FISMA audit report.

(U) Continuous Monitoring Maturity Model

(U) As part of the updated FY 2015 DHS FISMA reporting metrics, dated June 19, 2015, the Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE), DHS, OMB, NIST, and other stakeholders developed a maturity model for the continuous monitoring domain to provide perspective on the overall status of information security within an agency. The purpose of the CIGIE maturity model is to:

- **(U)** Summarize the status of agencies' information security programs and their maturity on a 5-level scale (details are included in Appendix C);
- **(U)** Provide transparency to agency chief information officers, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level; and
- **(U)** Help ensure consistency across the OIGs in their annual FISMA reviews.

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

(U) AUDIT RESULTS

~~(SBU)~~ Finding A: USIBWC Effectively Implemented Security Programs and Related Practices for Its General Support System

~~(SBU)~~ OIG found that USIBWC generally implemented an information security program and related practices with effective security controls for configuration management, continuous monitoring,[4] identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, and contingency planning for its general support system (GSS).[5] OIG further reviewed access controls and personnel security and found that USIBWC implemented effective security controls for these areas. For physical and environmental protection, OIG found that USIBWC conducted physical and environmental self-assessments in FY 2015 [Redacted] (b) (5) USIBWC documented identified vulnerabilities from the physical and environmental self-assessments with associated corrective actions/remediation activities planned to improve security controls. In addition, USIBWC defined comprehensive policies, procedures, and strategies consistent with NIST and OMB requirements for its GSS. The program and activities for the GSS were consistently applied across the organization, and USIBWC used metrics to measure and manage the program and activities.

~~(SBU)~~ Finding B: [Redacted] (b) (5)

~~(SBU)~~ OIG found that USIBWC has not implemented an effective [Redacted] (b) (5) procedure for its [redacted] NIST Special Publication (SP) 800-53, Revision 4,[6] states that the organization "Develops, documents, and disseminates…Procedures to facilitate the implementation [Redacted] (b) (5) Although USIBWC had [Redacted] (b) (5) policy and procedures for its GSS, the procedures could not be applied to [Redacted] (b) (5) [Redacted] (b) (5) for the [redacted] requires expertise to implement a change without affecting the system's high availability[7] and sensitivity requirements. Because USIBWC did not have the in-house expertise [Redacted] (b) (5), it executed a contract with [redacted] to design and implement an upgrade strategy for its [Redacted] (b) (5)

[4] (U) [Redacted] (b) (5)

[5] (U) According to NISTIR (Interagency Report) 7298, rev. 2, May 2013, "Glossary of Key Information Security Terms," a general support system is "An interconnected set of information resources under the same direct management control… . It normally includes hardware, software, information, data, applications, communications, and people."

[6] (U) NIST SP 800-53, rev. 4, [redacted] Apr. 2013.

[7] (U) According to NIST SP 800-34, rev. 1, Nov. 2010, "Contingency Planning Guide for Federal Information Systems," "[High Availability] is a process where redundancy and failover processes are built into a system to maximize its uptime and availability."

~~(SBU)~~ According to USIBWC officials, the upgrade design strategy for the [Redacted] (b) (5) has recently been completed and testing of controls is expected to be completed by the end of September 2015. Further, the [Redacted] (b) (5) upgrade design strategy is in final draft and USIBWC acceptance of the design is scheduled for the end of October 2015. USIBWC expects the solicitation for implementation of the upgrade design strategy before the end of 2015 with full implementation expected to be completed by June 2016. [as part of the

[Redacted] (b) (5)

~~(SBU)~~ Figure 2: [
(Photo taken by OIG)

~~(SBU)~~ USIBWC has not fully implemented [Redacted] (b) (5) for its [Redacted] (b) (5) due to the time required to award a contract and implement a [Redacted] (b) (5) upgrade design strategy. Until USIBWC fully implements its [Redacted] (b) (5) upgrade and planned [Redacted] (b) (5) [Redacted] (b) (5) could compromise the confidentiality, integrity, and availability of the systems. For example, USIBWC has taken steps to mitigate the [Redacted] (b) (5) to vulnerabilities using an [Redacted] (b) (5) until a more permanent solution is implemented. However, the [Redacted] (b) (5)

[Redacted] (b) (5)

[Redacted] (b) (5) which leaves the [Redacted] (b) (5) systems vulnerable to security weaknesses.

~~(SBU)~~ **Recommendation 1:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, complete the implementation of its upgrade design and planned improvements to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.

~~(SBU)~~ **USIBWC Response:** USIBWC concurred with this recommendation, stating that it had implemented and substantially completed the upgrade design strategy for [Redacted] (b) (5) in FY 2015, which included implementation of all [Redacted] (b) (5) controls found within NIST 800-53. According to USIBWC, an Authority to Operate package is being finalized and will be provided to the U.S. Commissioner in October 2015. A contract to implement an upgrade design of the will be awarded in October 2015, with full implementation of the [Redacted] (b) (5) upgrade expected to be completed by July 2016. This upgrade will also include the implementation of [Redacted] (b) (5) controls found within NIST 800-53.

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that USIBWC has completed implementation of its [Redacted] (b) (5) upgrade design and [Redacted] (b) (5)

~~(SBU)~~ Finding C: [Redacted] (b) (5)

(U) NIST SP 800-53, rev. 4,[10] states that organizations should establish a [Redacted] (b) (5)

~~(SBU)~~ Although OIG found that USIBWC had an effective [Redacted] (b) (5) for its GSS, [Redacted] (b) (5) Specifically, OIG found that USIBWC developed, with assistance from [Redacted] (b) (5) an upgrade design strategy [Redacted] (b) (5) at the [Redacted] (b) (5)

[10] (U) NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," [Redacted] (b) (5)

[11] (U) NIST SP [Redacted] (b) (5)

in [Redacted] (b) (5) The upgrade strategy defines[12] a [Redacted] (b) (5) However, at the time of our site visit in April 2015, the upgrade strategy had not been fully implemented[14] [Redacted] (b) (5) According to USIBWC officials, an upgrade strategy [Redacted] (b) (5) was completed and final testing of the controls is expected by the end of September 2015.

~~(SBU)~~ In addition, an upgrade design strategy was also completed for the [Redacted] (b) (5), which included the implementation of . USIBWC acceptance of the design is scheduled for the end of October 2015. USIBWC expects full implementation [Redacted] (b) (5) by June 2016.

~~(SBU)~~ USIBWC has not fully implemented because of the technical resources and time required to implement the upgrade strategy. Without a fully implemented [Redacted] (b) (5) program, there is increased risk that threats and vulnerabilities may go undetected, which could lead to potential damage or disruption to services provided by the [Redacted] (b) (5)

~~(SBU)~~ USIBWC implemented [Redacted] (b) (5) based on the criteria established in the CIGIE ISCM Maturity Model.[15] USIBWC implemented a standardized and defined for its GSS with policies, procedures, and strategies. However,) was not implemented across the organization because it has not yet been applied to For [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 2:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement [Redacted] (b) (5) as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, [Redacted] (b) (5)

[Redacted] (b) (5)

[15] **(U)** DHS FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2," by U.S. Department of Homeland Security, Jun. 19, 2015.

~~(SBU)~~ **USIBWC Response:** USIBWC concurred with this recommendation, stating that it has completed the upgrade [Redacted] (b) (5) USIBWC has also finalized an upgrade design strategy [Redacted] (b) (5) The award for the upgraded design is scheduled for October 2015, with full implementation expected to be completed by July 2016.

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that USIBWC has completed implementation of [Redacted] (b) (5).

~~(SBU)~~ Finding D: [Redacted] (b) (5)

~~(SBU)~~ USIBWC owns the [Redacted] (b) (5) [Redacted] (b) (5) and the facility uses a that is operated by a contractor [Redacted] (b) (5) [Redacted] (b) (5) on USIBWC's behalf. Agencies are required to oversee contractor-operated systems to ensure they are compliant with FISMA.[16]

~~(SBU)~~ The current [Redacted] (b) (5) operation and maintenance contract does not include provisions to ensure that the contractor-operated [Redacted] (b) (5) has effective security controls that are compliant with FISMA. For example, the current contract does not require [Redacted] (b) (5) [Redacted] (b) (5) to perform FISMA required[17] [Redacted] (b) (5) USIBWC issued contract modifications [Redacted] (b) (5) with the intent to have the contractor assist USIBWC in reaching FISMA compliance. However, on July 23, 2015, USIBWC informed OIG that these efforts resulted in only some improvements towards meeting FISMA security requirements. According to USIBWC officials, they now believe that the most efficient and effective solution to bring the [Redacted] (b) (5) into FISMA compliance is to implement a [Redacted] (b) (5) upgrade strategy, similar to the strategy used [Redacted] (b) (5).

~~(SBU)~~ [Redacted] (b) (5) The [Redacted] (b) (5) operation and maintenance contract that was re-awarded to [Redacted] (b) (5) became effective [Redacted] (b) (5) The contract requires the contractor to add a dedicated [Redacted] (b) (5) systems analyst to their existing staff to assist USIBWC in reaching and maintaining FISMA compliance. Because the present

[16] **(U)** Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, section 3553, "Authority and functions of the Director and the Secretary," (a)(1) and (a)(2)(B), states: "The Director shall oversee agency information security policies and practices including…information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."

[17] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," Apr. 2013, [Redacted] (b) (5).

[Redacted] (b) (5) is not compliant with FISMA, it is susceptible to outside attacks and insider threats.

~~(SBU)~~ **Recommendation 3:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, ensure its contractor-operated [Redacted] (b) (5) [Redacted] (b) (5) [Redacted] (b) (5) complies with the Federal Information Security Management Act.

~~(SBU)~~ **USIBWC Response:** USIBWC concurred with this recommendation, stating that it issued several modifications to the Operation and Maintenance contract, requiring the contractor to comply with FISMA security requirements. A contract to implement the full [Redacted] (b) (5) upgrade strategy based on successes at the [Redacted] (b) (5) [Redacted] (b) (5) [Redacted] (b) (5) is expected to be issued in October 2015. Lastly, the new Operation and Maintenance contract requires the contractor to have a dedicated [Redacted] (b) (5) systems analyst to respond to all FISMA requirements.

~~(SBU)~~ **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that USIBWC completed implementation of the full [Redacted] (b) (5) upgrade strategy at [Redacted] (b) (5) and the [Redacted] (b) (5) systems analyst position has been employed at [Redacted] (b) (5) to respond to all FISMA requirements.

(U) See Appendix D for the complete text of USIBWC's response to the recommendations.

(U) RECOMMENDATIONS

~~(SBU)~~ **Recommendation 1:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, complete the implementation of its [Redacted] (b) (5) upgrade design and planned [Redacted] (b) (5) improvements [Redacted] (b) (5) systems to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.

~~(SBU)~~ **Recommendation 2:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement a [Redacted] (b) (5) systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, [Redacted] (b) (5).

~~(SBU)~~ **Recommendation 3:** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, ensure its contractor-operated [Redacted] (b) (5) [Redacted] (b) (5) complies with the Federal Information Security Management Act.

(U) See Appendix D for the complete text of USIBWC's response to the recommendations.

(U) APPENDIX A: SCOPE AND METHODOLOGY

(U) The Federal Information Security Management Act of 2002 (FISMA), amended by the Federal Information Security Modernization Act of 2014, Public Law 113-283, 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 and the Department of Homeland Security (DHS). The FY 2015 FISMA guidance from DHS is intended to assist Offices of Inspector General (OIG) in reporting FISMA performance metrics. The updated FY 2015 DHS FISMA reporting metrics dated June 19, 2015, included the Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency maturity model for the continuous monitoring domain to provide perspective on the summary of the status of the agency's information security continuous monitoring program on a 5-level scale.

(U) OIG conducted this audit to assess the effectiveness of the International Boundary and Water Commission, United States and Mexico, U.S. Section's (USIBWC) information security program in FY 2015. Specifically, OIG assessed USIBWC's information security program and related practices for risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring, contingency planning, oversight of contractor systems, access controls, personnel security, and physical and environmental protection.

(U) OIG, Office of Audits, performed this audit from April 2015 through September 2015. OIG performed site visits to the USIBWC headquarters in El Paso, TX; [Redacted] (b) (5) [redacted] and the General Support System continuity of operations site in Las Cruces, NM.

(U) OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on its audit objective. OIG believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

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

OIG assessed the data reliability for data extracted from USIBWC databases, Microsoft Excel spreadsheets, Microsoft Access reports, and enterprise software application reports.

(U) Prior Reports

~~(SBU)~~ OIG reviewed prior OIG FISMA audit and evaluation reports to identify information previously reported relating to the USIBWC information security programs. OIG has conducted an annual FISMA audit of the information security program for the USIBWC since FY 2011. In the FY 2013 USIBWC annual FISMA report,[1] OIG issued 27 recommendations to improve USIBWC information security programs related to FISMA. In 2014,[2] USIBWC closed 22 of 27 recommendations, while 5 recommendations from the FY 2013 report were reissued. In addition, OIG issued one new recommendation.

(U) Work Related to Internal Controls

~~(SBU)~~ OIG performed steps to assess the adequacy of internal controls related to the areas audited. For example, OIG gained an understanding of the effectiveness of USIBWC's information security program as required by FISMA. OIG gained an understanding of internal controls consistent of USIBWC's information systems through its policies, procedures, and processing related to continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, access controls, personnel security, and physical and environmental protection. OIG's conclusions are presented in the Audit Results section of this report.

(U) Use of Computer-Processed Data

~~(SBU)~~ In the course of this audit, USIBWC provided computer-processed data,[3] which included data extracted from USIBWC databases, Microsoft Excel, Microsoft Access, and reports from enterprise software applications. OIG relied primarily on data provided from the USIBWC Information Management Division. To assess the data reliability, OIG performed tests of appropriateness[4] that entailed reviews and comparisons of data against other sources of information, as well as interviews with USIBWC Information Management Division officials who are responsible for compiling these data. OIG determined that the data were sufficiently reliable to support the conclusions and recommendations presented in this report.

---

[1] **(U)** *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD-IT-13-39, Sept. 2013).

[2] **(U)** *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD-IT-14-33, Sept. 2014).

[3] **(U)** GAO-09-680G, "Assessing the Reliability of Computer-Processed Data," dated Jul. 2009, defines computer-processed data as data entered into a computer system or results from computer processing.

[4] **(U)** GAO-09-680G, "Assessing the Reliability of Computer-Processed Data," dated Jul. 2009, "Appropriateness includes validity and reliability…completeness and accuracy of the data."

(U) Detailed Sampling Methodology

~~(SBU)~~ OIG's sampling objective was to test the effectiveness of the USIBWC implementation of information system security controls. Specifically, OIG wanted to assess information system security controls related to USIBWC risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring, contingency planning, oversight of contractor systems, access controls, personnel security, and physical and environmental protection.

~~(SBU)~~ To achieve the sampling objective, OIG selected a sample of information technology equipment to audit from the universe of USIBWC's IT equipment inventory. To select the sample, OIG used U.S. Government Accountability Office/President's Council on Integrity and Efficiency (GAO/PCIE) Financial Audit Manual 450 guidelines.[5] According to those guidelines, for a population exceeding 2,000 items, a sample size of 45 items would ensure that the control is operating effectively. As USIBWC's inventory consisted of approximately 2,300 items, OIG used a sample size of 45 items for testing. The items were randomly selected from USIBWC's inventory records using Microsoft Excel's random number generator. In addition, during our site visits to USIBWC headquarters, [redacted] OIG selected IT equipment on-site to determine if they were accurately recorded in applicable inventory records.

[5] **(U)** GAO/PCIE Financial Audit Manual, dated Jul. 2008, section 450.07, "Sample Size."

~~(SBU)~~ APPENDIX B: OFFICE OF INSPECTOR GENERAL FY 2014 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT STATUS OF RECOMMENDATIONS

~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission establish and implement a [Redacted] (b) (5) strategy for the International Boundary and Water Commission [Redacted] (b) (5) systems as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ *Status: This recommendation has been reissued, with revision to address the progress made relating to the* [Redacted] (b) (5) *systems at the* [redacted] *s Recommendation 2 (Finding C) of the FY 2015 report and closed in the FY 2014 Federal Information Security Management Act (FISMA) report.*

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) policy for its [redacted] systems to include [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ *Status: This recommendation has been reissued, with revision to address the progress made relating to* [Redacted] (b) (5) *as Recommendation 1 (Finding B) of the FY 2015 report and closed in the FY 2014 FISMA report.*

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-82.

(U) *Status: Closed July 2015.* OIG combined and reissued this recommendation as part of Recommendation 1 (Finding B) within the FY 2015 International Boundary and Water Commission, United States and Mexico, U.S. Section FISMA report.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5), as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

(U) *Status: Closed July 2015.* International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC) tested the contingency plan for its General Support System.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission ensure its contractor-operated [Redacted] (b) (5)

~~(SBU)~~ *Status: This recommendation has been reissued, with revision to address the progress made relating to the* [Redacted] (b) (5) *system at* [Redacted] (b) (5) *as Recommendation 3 (Finding D) of the FY 2015 report and closed in the FY 2014 FISMA report.*

~~(SBU)~~ **Recommendation 6.** OIG recommends that the International Boundary and Water Commission (USIBWC) determine ownership of information technology inventory and update the Integrated Logistics Management System to accurately reflect USIBWC's current information system components, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed July 2015.* USIBWC has determined ownership of information technology inventory and updated the Integrated Logistics Management System to accurately reflect USIBWC's current information system components.

(U) APPENDIX C: INSPECTOR GENERAL INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) MATURITY MODEL FOR FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT ACT

(U) Level	(U) Definition
1 Ad-hoc	**(U) ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • **(U)** ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • **(U)** ISCM stakeholders and their responsibilities have not been defined and communicated across the organization. • **(U)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • **(U)** The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities. • **(U)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. • **(U)** The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. • **(U)** ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. • **(U)** There is no defined process for collecting and considering lessons learned to improve ISCM processes. • **(U)** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

(U) Level	(U) Definition
2 Defined	**(U) The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.** • **(U)** ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • **(U)** ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities. • **(U)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • **(U)** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. • **(U)** The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective. • **(U)** The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities. • **(U)** The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements. • **(U)** ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.

(U) Level	(U) Definition
3 Consistently Implemented	**(U) In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • **(U)** The ISCM program is consistently implemented across the organization, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • **(U)** ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties. • **(U)** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. • **(U)** The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools are interoperable, to the extent practicable. • **(U)** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. • **(U)** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. • **(U)** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.
4 Managed and Measurable	**(U) In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.** • **(U)** Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes. • **(U)** Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • **(U)** ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations. • **(U)** ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response. • **(U)** ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a

(U) Level	(U) Definition
	threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains. • **(U)** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis
5 Optimized	**(U) In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.** • **(U)** Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. • **(U)** The ISCM program is integrated with strategic planning, enterprise architecture, and capital planning and investment control processes. • **(U)** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.

(U) Source: Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics.*

(U) APPENDIX D: INTERNATIONAL BOUNDARY AND WATER COMMISSION, UNITED STATES AND MEXICO, U.S. SECTION, MANAGEMENT RESPONSE

INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

October 16, 2015

Mr. Norman P. Brown
United States Department of State
Assistant Inspector General for Audits
Office of Inspector General
Washington, D. C. 20520

Subject: Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program, AUD-IT-16-XX

Dear Mr. Brown:

We received and have reviewed the draft report "Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program". Thank you for the opportunity to comment on your draft audit recommendations.

Below please find our responses to each of the recommendations as requested. Please advise if you have any questions or if we may be of any assistance.

Sincerely,

Edward Drusina, P.E.
Commissioner

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

~~(SBU)~~ Finding B: [Redacted] (b) (5)

~~(SBU)~~ Recommendation 1: OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, complete the implementation of its [Redacted] (b) (5) upgrade design and planned [Redacted] (b) (5) improvements [Redacted] (b) (5) systems to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.

~~(SBU)~~ Management Response: Concur. An upgrade design strategy for the [Redacted] (b) (5) [Redacted] (b) (5) system was implemented and substantially completed in FY15. An Authority to Operate (ATO) package is being finalized and will be submitted to the U.S. Commissioner in October 2015. The upgraded system includes the implementation of all [Redacted] (b) (5) controls found within the NIST 800-53 [Redacted] (b) (5). A contract to implement an upgrade design of the [Redacted] (b) (5) system will be awarded in October 2015, which will also include the implementation of all [Redacted] (b) (5) controls found within the NIST 800-53 [Redacted] (b) (5) [Redacted] (b) (5). Full implementation of the [Redacted] [Redacted] (b) (5) system upgrade is expected to be completed by July 2016.

~~(SBU)~~ Finding C: [Redacted] (b) (5) [Redacted] (b) (5)

~~(SBU)~~ Recommendation 2: OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement a [Redacted] (b) (5) as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, [Redacted] (b) (5)

~~(SBU)~~ Management Response: Concur. An upgrade for the [Redacted] (b) (5) system has been completed. This new system has implemented a [Redacted] solution in response to this audit finding. Similarly, an upgrade design strategy has also been finalized for the [Redacted] (b) (5) [Redacted] (b) (5) system, which includes the implementation of [Redacted] (b) (5). The award of the upgraded design is scheduled for October 2015. Full implementation of the [Redacted] (b) (5) [Redacted] (b) (5) system upgrade is expected to be completed by July 2016. Upon completion of this project, the USIBWC will have a robust [Redacted] (b) (5) systems, as required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, rev. 4 and outlined in [Redacted] (b) (5).

~~(SBU)~~ Finding D: [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, ensure its contractor-operated [Redacted] (b) (5) [Redacted] (b) (5) complies with the Federal Information Security Management Act.

~~(SBU)~~ **Management Response: Concur.** The USIBWC issued several mods to the O&M contract, which requires the contractor to comply with FISMA security requirements. A contract will be issued in October 2015 to implement the full [Redacted] (b) (5) [Redacted] (b) (5) upgrade strategy based on the successes at the [Redacted] (b) (5). Lastly, the new O&M contract requires the contractor to have a dedicated Information Technology position, [Redacted] (b) (5) Systems Analyst [Redacted] (b) (5) to respond to all FISMA requirements. The new contract is projected to be in place by October 2015. All prior mods issued to the Operations and Maintenance contract have been executed, which requires the contractor to fully comply with FISMA.

(U) ABBREVIATIONS

CIGIE	Council of Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
GSS	General Support System
IBWC	International Boundary and Water Commission
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
[Redacted] (b) (5)	[Redacted] (b) (5)
OIG	Office of Inspector General
OMB	Office of Management and Budget
[Redacted] (b) (5)	[Redacted] (b) (5)
[Redacted] (b) (5)	[Redacted] (b) (5)
SP	Special Publication
USIBWC	International Boundary and Water Commission, United States and Mexico, U.S. Section

(U) OIG AUDIT TEAM

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Steve Matthews, IT Audit Manager
Information Technology Division
Office of Audits

Sunlon Ung, Senior IT Auditor in Charge
Information Technology Division
Office of Audits

Doug Hundley, Senior Auditor
Information Technology Division
Office of Audits

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

OIGWPEAOmbuds@state.gov