OIG
Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

AUD-IT-16-46 | Office of Audits | August 2016

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

INFORMATION TECHNOLOGY DIVISION

OIG HIGHLIGHTS

AUD-IT-16-46

August 2016
OFFICE OF AUDITS
Information Technology Division

(U) Audit of the 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 and whether security practices in FY 2016 complied with laws and regulations established by the Federal Information Security Management Act of 2002 (FISMA), as amended, and standards prescribed by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

(U) In addition, OIG collected information from USIBWC regarding computer security controls for personally identifiable information (PII), as required by the Consolidated Appropriations Act, 2016, Section 406, Federal Computer Security.

(U) What OIG Recommends

(U) In the 2015 FISMA audit report, OIG made three recommendations to address the deficiencies identified during the audit. At the conclusion of fieldwork for this audit, these recommendations remained open, and OIG is making three additional recommendations in this report related to protecting PII and incident response. OIG provided USIBWC a draft of this report and requested comments, but USIBWC did not respond within the timeframe allotted for this mandated audit. Therefore, OIG considers all three newly issued recommendations unresolved, pending further action, and will monitor the implementation of all six recommendations in this report during the audit compliance process.

(U)What OIG Found:

~~(SBU)~~ During FY 2016, USIBWC maintained an effective information security program for its General Support System; however, OIG found that USIBWC has not implemented controls to ensure the confidentiality and integrity of PII saved on its General Support System. Specifically, USIBWC has not deployed an encryption method to protect PII residing on its servers. Further, USIBWC has not published a notice of the Systems of Records, as required by the Privacy Act. Without adequate protection of PII data, there is increased risk that unauthorized disclosure of PII could occur.

~~(SBU)~~ OIG also found that additional actions are needed to fully secure USIBWC's Supervisory Control and Data Acquisitions (SCADA) systems. Although USIBWC is taking action to improve [redacted] and FISMA compliance for its SCADA systems, as of March 2016, when OIG performed fieldwork for this audit, USIBWC had not fully implemented the improvements. According to USIBWC officials, the improvements should generally be implemented during 2016. Until an upgrade strategy, [redacted] improvements are implemented, the confidentiality, integrity, and availability of the SCADA systems will remain at increased risk.

~~(SBU)~~ OIG is also reporting required information related to USIBWC's computer security controls for covered systems. OIG provided information on USIBWC's logical access controls and practices as well as multi-factor authentication. OIG found that USIBWC established and maintained an inventory of systems but did not implement data loss prevention or digital rights management technological solutions.

Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

CONTENTS

(U) OBJECTIVE 1
(U) BACKGROUND 2
(U) The Federal Information Security Modernization Act of 2014 3
(U) FY 2016 FISMA Reporting Metrics 4
(U) Maturity Models 4
(U) Consolidated Appropriations Act, 2016, Section 406 5
(U) USIBWC's Personally Identifiable Information and National Security Systems 6
(U) AUDIT RESULTS 6
(U) Finding A: USIBWC Effectively Implemented Security Programs and Related Practices for its General Support System 6
~~(SBU)~~ Finding B: [redacted] Systems Has Not Been Implemented 8
~~(SBU)~~ Finding C: [redacted] Systems Has Not Been Implemented 10
~~(SBU)~~ Finding D: [redacted] Systems Has Not Been Implemented 12
~~(SBU)~~ Finding E: USIBWC Contractor-Operated [redacted] System at SBIWTP Is Not FISMA Compliant 13
(U) RECOMMENDATIONS 15
(U) APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY 16
(U) Prior Reports 17
(U) Work Related to Internal Controls 18
(U) Use of Computer-Processed Data 18
(U) Detailed Sampling Methodology 18
~~(SBU)~~ APPENDIX B: OFFICE OF INSPECTOR GENERAL FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT STATUS OF RECOMMENDATIONS 20
(U) APPENDIX C: INSPECTOR GENERAL INFORMATION SECURITY CONTINUOUS MONITORING MATURITY MODEL FOR FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 21
(U) APPENDIX D: INSPECTOR GENERAL COMPUTER SECURITY INCIDENT RESPONSE MATURITY MODEL FOR FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 27
(U) APPENDIX E: CONSOLIDATED APPROPRIATIONS ACT, 2016, SECTION 406, FEDERAL COMPUTER SECURITY 35
(U) Section A. Logical Access Policies and Practices 35
(U) Section B. Logical Access Controls for Privileged Users and Multi-Factor Authentication for Privileged Users 44

(U) Section C. Reasons for Not Having Minimum Logical Access Controls and Multi-Factor Authentication for Privileged Users 46

(U) Section D. Other Information Security Management Practices 46

(U) Section E. Entities That Provide Services to the International Boundary and Water Commission, United States and Mexico, U.S. Section 47

(U) ABBREVIATIONS 49

(U) OIG AUDIT TEAM MEMBERS 50

(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 (USIBWC), information security program and whether security practices in FY 2016 complied with laws and regulations established by the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, and standards prescribed by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). See Appendix A for the purpose, scope, and methodology of this audit. Appendix B provides the status of the recommendations made in the FY 2015 report.

(U) Additionally, OIG collected information from USIBWC regarding computer systems for the following topics, as required by the Consolidated Appropriations Act, 2016,[1] Section 406, Federal Computer Security:

A. (U) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
B. (U) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
C. (U) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
D. (U) A description of the following information security management practices used by the covered agency regarding covered systems:
    i. (U) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
    ii. (U) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –
        I. (U) data loss prevention capabilities;
        II. (U) forensics and visibility capabilities; or
        III. (U) digital rights management capabilities.
    iii. (U) A description of how the covered agency is using the capabilities described in clause (ii).
    iv. (U) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.
E. (U) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph D.

[1] (U) Public Law 114-113, 129 Stat. 2935, Cybersecurity Act of 2015.

(U) BACKGROUND

(U) The International Boundary and Water Commission is a binational commission created by the Convention of 1889.[2] The International Boundary and Water Commission is responsible for applying the boundary and water treaties between the United States and Mexico. The Commission 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 or her respective President. USIBWC is a Federal government agency that has its headquarters in El Paso, Texas. USIBWC operates under the foreign policy guidance of the U.S. Department of State (Department). The Mexican Section has its headquarters 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 do the following:

- **(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)** Preserve the boundary in the area bordering the Rio Grande and Colorado Rivers.
- **(U)** Demarcate the land boundary.

(U) USIBWC owns the contractor-operated South Bay International Wastewater Treatment Plant[3] (SBIWTP), located at San Diego, CA, which is responsible for meeting the Clean Water Act requirements mandated by the state of California. The SBIWTP discharges clean water into the Pacific Ocean. USIBWC also maintains and operates the Nogales International Wastewater Treatment Plant, located at Nogales, AZ, in accordance with the Clean Water Act requirements mandated by the state of Arizona.

(U) Each international wastewater treatment plant has a Supervisory Control and Data Acquisitions (SCADA)[4] system. The USIBWC SCADA systems are used to control dispersed assets

[2] **(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 Rivers, U.S.-Mex., March 1, 1889, 26 Stat. 1512 (extended indefinitely by Article two of treaty signed February 3, 1944.) (59 Stat. 1219).

[3] **(U)** Wastewater treatment plants are identified as a critical infrastructure sector whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

[4] **(U)** According to NIST Special Publication (SP) 800-82, rev. 2, May 2015, "Guide to Industrial Control Systems (ICS) Security," SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator, thereby allowing near real time monitoring or control of an entire system from a central location.

through centralized data acquisition. According to 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) The Federal Information Security Modernization Act of 2014

(U) The Federal Information Security Modernization Act of 2014[5] (Modernization Act) amends FISMA.[6] The Modernization Act enacts several important updates to FISMA. Key requirements of FISMA are the following:

- **(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)** The development, documentation, and implementation of an agency-wide program to provide a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal agency information security programs.
- **(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 Modernization Act reorganizes the structure and responsibilities of the OMB Director and provides authority to the Secretary of the Department of Homeland Security (DHS) to administer the implementation of information policies and practices government-wide. In addition, the Modernization Act updates the responsibilities of agency heads to require that agency heads ensure the following:

- **(U)** Information security management processes are integrated with budgetary planning.
- **(U)** Senior agency officials, including chief information officers, carry out their information security responsibilities.
- **(U)** All personnel are held accountable for complying with the agency-wide information security program.

(U) FISMA assigns specific responsibilities to NIST, OMB, DHS,[7] 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 IT security risks to an acceptable level. To ensure the adequacy and

[5] **(U)** Public Law No. 113-283.

[6] **(U)** Public Law No. 107-347.

[7] **(U)** OMB Memorandum M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland (DHS)," July 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 DHS. DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

(U) FY 2016 FISMA Reporting Metrics

(U) OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2016 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officer Council. The OIG metrics are organized around the five information security functions outlined in NIST standards. Table 1 provides information on the security functions and related metrics detailed for FY 2016.

(U) Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2016 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2016 OIG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

(U) Source: FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.0.

(U) Maturity Models

(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, 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 FY 2016 IG FISMA Reporting Metrics, dated June 20, 2016,[8] continued that effort with the introduction of an Incident Response maturity model. The purposes of the Council of Inspectors General on Integrity and Efficiency maturity models are as follows:

- (U) Summarize the status of agencies' information security programs and their maturity on a 5-level scale (details are included in Appendices C and D).

[8] (U) FY 2016 Inspector General, Federal Information Security Modernization Act of 2014 Reporting Metrics V 1.0, dated June 20, 2016.

- **(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.
- **(U)** Help ensure consistency across the OIGs in their annual FISMA reviews.

(U) Metrics for those domains without an established maturity model are mapped to Maturity Model Indicators. These indicators will act as a steppingstone, allowing IGs to reach preliminary conclusions similar to those achievable with a fully developed model.

(U) Consolidated Appropriations Act, 2016, Section 406

(U) The Consolidated Appropriations Act, 2016,[9] Section 406, Federal Computer Security, enacted on December 18, 2015, requires Inspectors General from each covered agency[10] to provide a report containing a description of controls utilized by covered agencies to protect sensitive information maintained, processed, and transmitted by a covered system.[11] The Consolidated Appropriations Act requests a description of controls utilized by covered agencies to protect two types of data contained within covered systems: personally identifiable information (PII) data and national security data.

(U) OMB published Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007. OMB M-07-16 requires all Federal agencies to develop and implement various security and operational requirements that Federal agencies must adhere to in order to sufficiently protect PII.[12]

(U) For information systems that process, transmit, or contain PII, NIST published NIST Special Publication (SP) 800-53, rev. 4.[13] NIST SP 800-53 provides a catalog of security and privacy controls for Federal information systems and organizations. For example, NIST SP 800-53 provides a process for selecting information security controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.

(U) The information gathered from USIBWC related to computer systems is provided in Appendix E of this report.

---

[9] Public Law 114-113, 129 Stat. 2935, Cybersecurity Act of 2015.

[10] **(U)** According to Sec. 406, the term "covered agency" means an agency that operates a covered system.

[11] **(U)** According to Sec. 406, the term "covered system" shall mean a National Security System as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

[12] **(U)** OMB, Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 2007.

[13] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "AT-4 Security Training Records," January 2014.

(U) USIBWC's Personally Identifiable Information and National Security Systems

(U) USIBWC did not identify any specific applications on its General Support System (GSS) that had PII. However, USIBWC maintains PII in its GSS environment. Specifically, it maintained an Excel spreadsheet that contains names, Social Security numbers, and dates of birth of employees. The purpose of the GSS is to provide internet and network resources to internal users as well as to field office users. The GSS consists of a wide area network and local area network established in the headquarters office in El Paso, TX. In addition, there are local area networks in 13 field offices. USIBWC officials stated that the agency did not maintain any National Security Systems.

(U) AUDIT RESULTS

(U) Finding A: USIBWC Effectively Implemented Security Programs and Related Practices for its General Support System

(U) OIG found that USIBWC generally implemented an information security program and related practices with effective security controls for risk management and contractor systems, configuration management, identity and access management, security and privacy training, [redacted][14] incident response, and contingency planning for its GSS.[15] OIG further reviewed access controls and personnel security and found that USIBWC implemented effective security controls for these areas for the GSS. OIG also found that 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.

(U) However, OIG identified an instance where PII was not being encrypted. According to NIST SP 800-53, rev. 4,[16] "The information system protects the [*Selection (one or more): confidentiality; integrity*] of [Assignment: organization-defined information at rest]: the information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined information system components]".

[14] **(U)** Additional information on [redacted] is discussed in Finding C.
[15] **(U)** According to NIST-IR (Interagency Report) 7298, rev. 2, May 2013, "Glossary of Key Information Security Terms," a GSS is "An interconnected set of information resources under the same direct management control…. It normally includes hardware, software, information, data, applications, communications, and people."
[16] **(U)** NIST SP 800-53, rev. 4, "Transmission Confidentiality and Integrity," SC-8.

~~(SBU)~~ OIG found that USIBWC had not implemented controls to ensure the confidentiality and integrity of PII[17] data at rest[18] on USIBWC shared drives and network. The Safety and Security Division within USIBWC maintains a list of approximately 400 USIBWC employees (including past, present, and recently hired but not yet on board) with their names, Social Security numbers, and dates of birth. This list is a spreadsheet used to track the investigations of employees when the information is obtained from the Office of Personnel Management. The tracking document was created to help the Safety and Security Division stay informed of the status and progress of individuals' clearance process. This would be considered a system of record,[19] according to the Privacy Act.[20]

~~(SBU)~~ USIBWC had identity and access policy and procedures for IT access control for all general assets and operations; however, the policy and procedures do not identify methods to prevent the unauthorized disclosure and modification of PII data. In addition, USIBWC had not implemented an encryption method for protecting PII data stored on the USIBWC network. Further, USIBWC had not published a Systems of Records Notice for the spreadsheet with PII data, as required by the Privacy Act.

~~(SBU)~~ Because of USIBWC's lack of implementation of an encryption method for protecting data stored on USIBWC networks, there is increased risk that unauthorized disclosure of PII could occur. In addition, until an encryption method is implemented, names, Social Security numbers, and dates of birth are at risk for a data breach. PII is residing on servers that could be compromised because of the lack of controls protecting the data at rest.

Recommendation 1: (U) OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement encryption for its personally identifiable information stored on its shared drives and network to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.

(U) USIBWC Response: USIBWC did not provide a response to a draft of this report within the timeframe allotted.

(U) OIG Reply: Because USIBWC did not provide a response, OIG considers this recommendation unresolved. This recommendation will be resolved when USIBWC provides a plan of action for implementing the recommendation. This recommendation will be closed when OIG receives and accepts documentation demonstrating that USIBWC has

[17] **(U)** As defined by OMB M-07-16, PII refers to information that can be used to distinguish or trace an individual's identity, such as the individual's name, Social Security number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

[18] **(U)** Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

[19] **(U)** A system of record is a group of records from which information is retrieved by the name of an individual or by any number, symbol, or other unique identifier assigned to that individual.

[20] **(U)** Privacy Act of 1974 (5 U.S.C § 552a).

implemented encryption for its personally identifiable information stored on its shared drives and networks.

Recommendation 2: (U) OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, issue a Systems of Records Notice that addresses the privacy information collected, as required by the Privacy Act.

(U) USIBWC Response: USIBWC did not provide a response to a draft of this report within the timeframe allotted.

(U) OIG Reply: Because USIBWC did not provide a response, OIG considers this recommendation unresolved. This recommendation will be resolved when USIBWC provides a plan of action for implementing the recommendation. This recommendation will be closed when OIG receives and accepts documentation demonstrating that USIBWC has issued a Systems of Records Notice that addresses the privacy information collected.

~~(SBU)~~ Finding B: [redacted] for USIBWC [redacted] Has Not Been Implemented

~~(SBU)~~ OIG found USIBWC has not implemented an effective [redacted] USIBWC had a [redacted] policy and procedures for its GSS; however, the procedures could not be applied to its [redacted] to design an upgrade strategy for the [redacted], which includes improving [redacted] The upgrade strategy was in the implementation assessment phase[22] as of April 2016, the end of OIG's audit fieldwork. USIBWC planned to use a similar upgrade strategy to implement [redacted] According to USIBWC officials, the upgrade [redacted] was substantially completed by June 2016, which was after the end of fieldwork for this audit.

(SBU) During the FY 2016 audit, USIBWC stated that the [redacted] was still in the implementation phase for all [redacted] controls. USIBWC anticipated completing this effort earlier. However, according to USIBWC officials, USIBWC conducted an inspection of the contractor's work on this effort in August 2015. The inspection revealed that the contractor had not implemented certain requirements from the contract related to security controls and documentation; therefore, USIBWC refused to take ownership of the product at that time. Since then, USIBWC has been working with the contractor

[21] **(U)** According to NIST IR 7298, rev. 2, high availability is a failover feature to ensure availability during device or component interruptions.

[22] **(U)** According to NIST SP 800-64, rev. 2, Oct. 2008, "Security considerations in the System Development Life Cycle," section 3.3, Implementation/Assessment is the third phase of the System Development Life Cycle, during which the system will be installed and evaluated in the organization's operational environment.

to fully implement all required controls. USIBWC officials estimated that an official Authority to Operate designation will be provided in July 2016 for the [redacted] (which was after the end of fieldwork for this audit). This upgrade design strategy will be replicated at the [redacted] facility.

~~(SBU)~~ Until a [redacted] policy is implemented, changes to the [redacted] could compromise the confidentiality, integrity, and availability of the systems. For example, during audit fieldwork, [redacted]

(U) The FY 2015 report on USIBWC's information security program[23] contained a recommendation to address this deficiency; consequently, OIG is not making a new recommendation in this report. The recommendation and the status of the recommendation are as follows:

~~(SBU)~~ *Recommendation 1 (AUD-IT-16-07). OIG recommends that the U.S. Section of the International Boundary and Water Commission, United States and Mexico, complete the implementation of its* [redacted] *to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.*

~~(SBU)~~ *Status and OIG Reply (as of June 2016). Resolved. OIG acknowledges USIBWC's actions thus far to implement the recommendation; however, it has not provided OIG with documentation showing that the actions taken have been implemented. This recommendation will be closed when OIG receives and accepts documentation showing that USIBWC has completed implementation of its* [redacted]

~~(SBU)~~ *In June 2016, after OIG fieldwork was complete, USIBWC officials stated that an upgrade design strategy for the* [redacted] *system was implemented and substantially completed. USIBWC was finalizing an Authority to Operate package and planned to submit the package to the U.S. Commissioner. USIBWC officials anticipated that an official Authority to Operate designation for the* [redacted] *plant will be provided in July 2016.*

(U) *OIG Reply. Based on USIBWC's response in June 2016, this recommendation remains resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that USIBWC has applied the established procedures for* [redacted]

[23] **(U)** OIG, *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD-IT-16-07, October 2015).

~~(SBU)~~ Finding C: [redacted] Has Not Been Implemented

(U) NIST SP 800-53, rev. 4,[24] states that organizations should [redacted]

~~(SBU)~~ Although OIG found that USIBWC has an effective [redacted] for its GSS, [redacted] As of April 2015, OIG found that USIBWC developed, with assistance from TruShield Security Solutions, Inc., a system upgrade design strategy for [redacted] However, as of March 2016, the time of OIG's site visit to USIBWC, the upgrade strategy had not been fully implemented nor had [redacted] According to USIBWC officials, an upgrade strategy for the [redacted] was completed in June 2016, following OIG's audit fieldwork.

~~(SBU)~~ During OIG's site visit to USIBWC in April 2016, USIBWC planned to implement the same upgrade strategy for its [redacted] According to USIBWC officials, the upgrade design strategy was completed for the [redacted] which included the implementation of [redacted] capabilities. USIBWC expected full implementation of the [redacted] upgrade in 2016.

~~(SBU)~~ USIBWC has not fully implemented a [redacted] USIBWC anticipated completing this effort earlier. However, according to USIBWC officials, USIBWC conducted an inspection of the contractor's work on this effort in August 2015. The inspection revealed that the contractor had not implemented certain requirements from the contract related to security controls and documentation and that therefore USIBWC refused to take ownership of the product at that time. USIBWC had been working with the contractor to fully implement all controls. Without a fully implemented [redacted] program, there is increased risk [redacted]

~~(SBU)~~ OIG determined that USIBWC implemented an ISCM[26] at level [redacted] of 5, with 5 being the highest level of maturity, based on the criteria established in the Council of Inspectors General

[24] **(U)** NIST SP 800-53, rev. 4, [redacted]
[25] **(U)** NIST SP 800-[redacted]
[26] **(U)** See Appendix C for details of the Maturity Model.

on Integrity and Efficiency ISCM Maturity Model.[27] USIBWC maintained a standardized and defined ISCM automation for its GSS with policies, procedures, and strategies. [redacted] See Appendix C for details of level [redacted] requirements.

(U) The FY 2015 report on USIBWC's information security program[28] contained a recommendation to address this deficiency; consequently, OIG is not making a new recommendation in this report. The recommendation and the status of the recommendation are as follows:

~~(SBU)~~ *Recommendation 2 (AUD-IT-16-07). OIG recommends that the U.S. Section of the International Boundary and Water Commission, United States and Mexico,* [redacted] *as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, and outlined in NIST SP 80* [redacted]

~~(SBU)~~ *Status and OIG Reply (as of June 2016). Resolved. OIG acknowledges USIBWC's actions thus far to implement the recommendation; however, it has not provided OIG with documentation showing that these actions have been completed. This recommendation will be closed when OIG receives and accepts documentation showing that USIBWC has completed implementation of its* [redacted]

~~(SBU)~~ *In June 2016, after OIG fieldwork was completed, USIBWC officials stated that USIBWC had recently implemented* [redacted] *Further, USIBWC officials stated that a similar upgrade design is being implemented at* [redacted] *which will include a* [redacted] *program when complete. Currently, the* [redacted] *USIBWC officials expected full implementation of the* [redacted] *upgrade to be completed in 2016.*

(U) *OIG Reply. Based on USIBWC's response in June 2016, this recommendation remains resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that USIBWC has implemented* [redacted]

[27] **(U)** "FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0," June 20, 2016.

[28] **(U)** AUD-IT-16-07, October 2015.

~~(SBU)~~ Finding D: [redacted] Has Not Been Implemented

(U) NIST SP 800-61, rev. 2,[29] states automated detection capabilities include network-based and host-based Intrusion Detection and Prevention Systems, antivirus software, and log analyzers. Further, NIST SP 800-53. rev. 4,[30] states that organizations test [redacted]

~~(SBU)~~ Although USIBWC had an [redacted] process for its GSS, USIBWC has not consistently implemented an [redacted] USIBWC is unable to measure and obtain metrics on the effectiveness of its [redacted]

~~(SBU)~~ USIBWC has not fully implemented an [redacted] USIBWC expected full implementation of the [redacted] upgrades in 2016.

~~(SBU)~~ Until USIBWC completes its upgrade strategy for its [redacted] USIBWC is unable to [redacted]

~~(SBU)~~ Until USIBWC completes its upgrade strategy for the [redacted] of 5, based on the criteria established in the Council of Inspectors General on Integrity and Efficiency Maturity Model.[31] For USIBWC to reach a level [redacted] it needs to [redacted] See Appendix D for details of level [redacted] requirements.

Recommendation 3: (SBU) OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, [redacted]

[29] **(U)** NIST 800-61, rev. 2, "Computer Security Incident Handling Guide," August 2012.

[30] **(U)** NIST SP 800-53, rev. 4, IR-3, "Incident Response Testing."

[31] **(U)** "FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0."

(U) USIBWC Response: USIBWC did not provide a response to a draft of this report within the timeframe allotted.

~~(SBU)~~ OIG Reply: Because USIBWC did not provide a response, OIG considers this recommendation unresolved. This recommendation will be resolved when USIBWC provides a plan of action for implementing the recommendation. This recommendation will be closed when OIG receives and accepts documentation demonstrating that USIBWC has implemented [redacted]

~~(SBU)~~ Finding E: USIBWC Contractor-Operated [redacted] Is Not FISMA Compliant

~~(SBU)~~ USIBWC owns the [redacted] The facility uses a SCADA system that is operated by the contractor Veolia Water West Operating Services, Inc., on USIBWC's behalf. Agencies are required to oversee contractor-operated systems to ensure they are compliant with FISMA.[32]

~~(SBU)~~ The previous Veolia contract for [redacted] operation and maintenance did not include provisions to ensure that the contractor-operated SCADA system at [redacted] During FY 2016, OIG noted that USIBWC awarded a new contract to Veolia to address plant operations and a separate contract to Aitheras to perform [redacted] based on the upgrade for the [redacted] Although USIBWC had awarded the contract and the contractor had started to improve the [redacted] full implementation had not taken place as of [redacted] when OIG performed fieldwork. As a result, the USIBWC contractor-operated [redacted] and was susceptible to outside attacks and insider threats.

(U) The FY 2015 report on USIBWC's information security program[33] contained a recommendation to address this deficiency; consequently, OIG is not making a new recommendation. The recommendation and the status of the recommendation are as follows:

~~(SBU)~~ *Recommendation 3 (AUD-IT-16-07). OIG recommends that the U.S. Section of the International Boundary and Water Commission, United States and Mexico, ensure its contractor-operated* [redacted]

~~(SBU)~~ *Status and OIG Reply (as of June 2016). Resolved. OIG acknowledges USIBWC's actions thus far to implement the recommendation; however, it has not provided OIG with*

[32] **(U)** [redacted]

[33] **(U)** AUD-IT-16-07, October 2015.

documentation showing that corrective action has occurred. This recommendation will be closed when OIG receives and accepts documentation showing that USIBWC completed implementation of the [redacted]

~~(SBU)~~ *In June 2016, after OIG fieldwork was complete, USIBWC officials stated that a contract to implement a complete upgrade of the* [redacted] *which also includes the implementation of* [redacted] *USIBWC anticipated that the upgraded system would be fully implemented* [redacted]

(U) *OIG Reply. Based on USIBWC's response in June 2016, this recommendation remains resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the* [redacted]

(U) RECOMMENDATIONS

Recommendation 1: (U) OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement encryption for its personally identifiable information stored on its shared drives and network to comply with National Institute of Standards and Technology, Special Publication 800-53, rev. 4, requirements.

Recommendation 2: (U) OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, issue a Systems of Records Notice that addresses the privacy information collected, as required by the Privacy Act.

Recommendation 3: ~~(SBU)~~ OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, [redacted]

(U) APPENDIX A: PURPOSE, 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 (OMB) and the Department of Homeland Security (DHS).

(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 and whether security practices in FY 2016 complied with laws and regulations established by the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, and standards prescribed by OMB and the National Institute of Standards and Technology.

(U) Additionally, OIG gathered information from USIBWC regarding computer systems for the following topics as required by the Consolidated Appropriations Act, 2016,[1] Section 406, Federal Computer Security:

A. **(U)** A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
B. **(U)** A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
C. **(U)** If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
D. **(U)** A description of the following information security management practices used by the covered agency regarding covered systems:
    i. **(U)** The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
    ii. **(U)** What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –
        I. **(U)** data loss prevention capabilities;
        II. **(U)** forensics and visibility capabilities; or
        III. **(U)** digital rights management capabilities.
    iii. **(U)** A description of how the covered agency is using the capabilities described in clause (ii).

[1] **(U)** Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406.

iv. (U) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

E. (U) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph D.

(U) OIG, Office of Audits, performed this audit from March through July 2016. OIG performed a site visit to USIBWC headquarters in El Paso, TX. 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 objectives.

(U) To perform this audit, OIG interviewed USIBWC senior management and employees to evaluate managerial effectiveness and operational controls in accordance with National Institute of Standards and Technology and OMB guidance. OIG observed daily operations and collected written documents to supplement observations and interviews. OIG reviewed training certifications to determine whether USIBWC employees met training requirements. Additionally, OIG assessed the level of the security clearance obtained for certain employees. OIG reviewed the IT Inventory listing and matched the locations and asset tags to what had been recorded by USIBWC.

(U) OIG also interviewed USIBWC officials to gain an understanding of USIBWC's current information security policies and procedures relating to USIBWC's computer security controls for its General Support System (GSS). Further, OIG collected and reviewed relevant written documents relating to the GSS.

(U) Prior Reports

(U) 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,[2] OIG issued 27 recommendations to improve USIBWC information security programs related to FISMA. In 2014,[3] USIBWC closed 22 of 27 recommendations, while 5 recommendations from the FY 2013 report were reissued. In addition, OIG issued one new recommendation. In the FY 2015 report,[4] OIG reissued three

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

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

[4] (U) OIG, *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD-IT-16-07, November 2015).

recommendations with revisions to address the progress made by USIBWC relating to its SCADA Systems.

(U) Work Related to Internal Controls

(U) 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 related to USIBWC's information systems by reviewing its policies and procedures for risk management and contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring,[5] incident response, and contingency planning for its GSS. OIG's conclusions are presented in the Audit Results section of this report.

(U) Use of Computer-Processed Data

(U) During this audit, USIBWC provided computer-processed data, which included data extracted from USIBWC databases, Microsoft Excel, Microsoft Access, and reports from enterprise software applications. To assess the data reliability, OIG performed tests of appropriateness 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 was sufficiently reliable to support the conclusions and recommendations presented in this report. OIG did not test the data for completeness. OIG found the data to be sufficiently reliable to meet the objectives of this audit.

(U) Detailed Sampling Methodology

(U) OIG's sampling objective was to test the effectiveness of USIBWC's implementation of information system security controls. Specifically, OIG wanted to assess information system security controls related to USIBWC [redacted]

(U) To achieve the sampling objective, OIG selected a sample of USIBWC training records to ensure that USIBWC employees had received training on IT security issues. USIBWC provided a universe of 243 security training records. One individual's record was excluded since this individual was in Leave Without Pay status, thus reducing the universe to 242 records. Using a simple random sampling methodology, a sample of records for 83 employees was selected. OIG determined that all employees had completed the necessary training requirements within the annual reporting period.

[5] **(U)** Additional information on [redacted] is discussed in Finding C in this report.

(U) OIG also selected a sample of employees from USIBWC's suitability[6] list to ensure that USIBWC employees' security clearances were consistent with their roles and responsibilities. USIBWC provided a universe of 561 records. OIG reviewed the suitability list and excluded four duplicate names; as a result, the universe was reduced to 557. The audit team selected a random sample of records of 30 employees to review. OIG found the security clearance status and dates of the employees' sampled matched information reported in the Office of Personnel Management database.

(U) OIG also selected a sample of the inventory included on USIBWC's inventory list to test the effectiveness of USIBWC's implementation of information system security controls. USIBWC provided a universe of 1,327 systems for USIBWC Headquarters. OIG excluded any inventory items valued at less than $500, resulting in a universe of 571 items. The sample size of 129 was selected using a partially dollar-weighted sample design. In a partially dollar-weighted design, the dollar-weighted portion is combined with a random sampling design. Therefore, 50 percent of the sample design was dollar-weighted, and 50 percent was a simple random sampling design.

(U) OIG reviewed the physical IT inventory at USIBWC Headquarters to determine whether assets were accurately recorded. To ensure that the IT hardware inventory was accurate and complete, the audit team traced the inventory and was able to locate 87 of 107 sampled items. An additional 20 items on the inventory list were later identified as excess equipment that had been taken out of service.

[6] **(U)** As defined in USIBWC SD.I. 10031, Personnel Security and Suitability Directive, "Suitability is an individual's character, reputation, trustworthiness, and fitness for overall employment as related to the efficiency of the Federal service."

~~(SBU)~~ APPENDIX B: OFFICE OF INSPECTOR GENERAL FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT STATUS OF RECOMMENDATIONS

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

(U) *Status: This recommendation remains open and is considered resolved because the International Boundary and Water Commission, United States and Mexico, U.S. Section, (USIBWC), has taken actions to implement it.*

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, implement a [redacted] as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, and outlined in NIST SP 800-137.

(U) *Status: This recommendation remains open and is considered resolved because USIBWC has taken actions to implement it.*

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission, United States and Mexico, U.S. Section, ensure its [redacted]

(U) *Status: This recommendation remains open and is considered resolved because USIBWC has taken actions to implement it.*

(U) APPENDIX C: INSPECTOR GENERAL INFORMATION SECURITY CONTINUOUS MONITORING MATURITY MODEL FOR FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT

(U)Table C.1: Inspector General Information Security Continuous Monitoring Maturity Model for FY 2016

1 Ad-hoc	**Information Security Continuous Monitoring (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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, SP 800-137, Office of Management and Budget (OMB) M-14-03, and the Chief Information Officer (CIO) ISCM Concept of Operations (CONOPS).** • ISCM stakeholders and their responsibilities have not been defined and communicated across the organization. • The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge skills and abilities to successfully implement an effective ISCM program. • The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. • The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. • ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • 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. • The organization has not defined processes for collecting and considering lessons learned to improve ISCM processes. • 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.

	• The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
2 Defined	**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.** • ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, tools) to effectively implement ISCM activities. • The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. • The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. • 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. • ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • 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. • 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.

	• The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. • The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
3 Consistently Implemented	**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.** • ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and the stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. • The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. • 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. • ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. • ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. • The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization.

	• The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM process and activities. • 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. • The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. • 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. • The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
4 Managed and Measurable	**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.** • The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. • Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. • Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organizational risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. • The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measure across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. • Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. • ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains. • The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejections, or transfer.

	• ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. • 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 Plan of Action and Milestones) up to date on an ongoing basis. • The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. • The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. • The organization utilizes a Security Information and Event Management (SIEM) tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk.
5 Optimized	**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.** • The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. • The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity 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. • The ISCM program is integrated with strategic planning, enterprise architecture and capital planning and investment control processes. • The ISCM program achieves cost-effective IT security objectives and goals and influences decision-making that is based on cost, risk, and mission impact. • The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time.

- The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.

(U) Source: FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.0 issued on June 20, 2016.

(U) APPENDIX D: INSPECTOR GENERAL COMPUTER SECURITY INCIDENT RESPONSE MATURITY MODEL FOR FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT

(U)Table D.1: Inspector General Computer Security Incident Response Maturity Model for FY 2016

Level	Definition
1 Ad-hoc	**Incident response program is not formalized and incident response 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 Federal Information Security Management Act (FISMA) (including guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-83, NIST SP 800-61 rev. 2, NIST SP 800-53, Office of Management and Budget (OMB) M-16-03, OMB M-16-04, and the United States Computer Emergency Readiness Team (US-CERT) , Federal Incident Notification Guidelines).** • Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, Department of Homeland Security (DHS), and OMB for all incident response activities. • The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. • The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. • The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. • Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response preparation/planning, incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT.

Level	Definition
	• The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. • The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. • The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. • The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. o -Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools o -Aggregation and analysis, such as security information and event management products o -Malware detection such as anti-virus and antispam software technologies o -Information management such as data loss prevention o -File integrity tools • The organization has not defined how it will meet the defined Trusted Internet Connection security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points. • The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. • The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.
2 Defined	**The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-53, NIST SP 800-61 rev. 2, NIST SP 800-83, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide, tested, and regularly updated.** • ISCM Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the

Level	Definition
	designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. • The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. • The organization has defined a common threat vector taxonomy and how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. • The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. • Incident response processes have been fully defined for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. • The organization has fully defined but not consistently implemented its processes to collaborate with DHS and other parties as appropriate, to provide on-site technical assistance/surge resources/special capabilities for quickly responding to incidents. • The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. • The organization has defined its processes for collecting and considering lessons learned and incident data to improve security

Level	Definition

	controls and incident response processes. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the incident response program.
	• The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas.
	  ○ Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools.
	  ○ Aggregation and analysis, such as security information and event management products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.
	  ○ Malware detection such as anti-virus and antispam software technologies.
	  ○ Information management such as data loss prevention.
	  ○ File integrity tools.
	However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable and have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.
	• The organization has defined how it will meet the defined Trusted Internet Connection security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points. However, the organization has not ensured that the Trusted Internet Connection 2.0 provider and agency managed capabilities are consistently implemented.
	• The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks.
	• The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems.

3 Consistently Implemented	**In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-53, NIST SP 800-61 rev. 2, NIST SP 800-83, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, measures and metrics on the effectiveness of the**

Level	Definition
	incident response program across the organization are not captured and utilized to make risk-based decisions and timely improvements to the program. • Incident response stakeholders and their responsibilities have been identified and communicated across the organization (Level 2). In addition, incident response teams and security operations centers, as appropriate, have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. • The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. • The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. • Incident response activities are fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. • Incident response processes are consistently performed across the organization for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. • The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. • The organization is consistently capturing qualitative and quantitative performance measures and metrics on the performance of its incident response program and is using the metrics to perform trend analysis, achieve situational awareness, and control ongoing risk. • The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. Lessons learned are consistently shared across the organization and used to make timely improvements to the incident response program and security measures. • The rigor, intensity, scope, and results of incident response activities (i.e., preparation, detection, analysis, containment, eradication, and

Level	Definition

	recovery, reporting, and post incident) are comparable and predictable across the organization.
	• The organization has consistently implemented its defined incident response technologies in the following areas.
	  ○ Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
	  ○ Aggregation and analysis, such as security information and event management products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors.
	  ○ Malware detection such as Anti-virus and antispam software technologies.
	  ○ Information management such as data loss prevention.
	  ○ File integrity tools.
	In addition, the tools are interoperable to the extent practicable and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.
	• The organization has consistently implemented defined Trusted Internet Connection security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points.
	• The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks.
	• The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems.

4 Managed and Measurable	**In addition to being consistently implemented (Level 3), incident response activities are repeatable and measures and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.** • Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. • Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program.

Level	Definition
	• Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. • The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. • Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. • Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations. • Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. • The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. • The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network.

Level	Definition
5 Optimized	**In addition to being managed and measurable (Level 4), the organization s incident response 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.** • The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. • The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. • On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. • The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. • The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. • The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. • The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. • The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly.

(U) Source: FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.0 issued on June 20, 2016.

(U) APPENDIX E: CONSOLIDATED APPROPRIATIONS ACT, 2016, SECTION 406, FEDERAL COMPUTER SECURITY

(U) Section A. Logical Access Policies and Practices

(U) *The Act requires the Inspector General to provide a description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.*

(U) Agency-wide Logical Access Control Policies

(U) The agency-wide "IT Access Control" policy establishes access controls for IT assets owned and operated by the International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC) and its personnel. This policy serves as USIBWC's framework by which access to information and information assets are issued, monitored, and maintained.

(U) As of June 2016, USIBWC is drafting a personally identifiable information (PII) handbook for safeguarding PII, which is anticipated to include administrative, technical, and physical safeguards to prevent unauthorized PII disclosure.

(U) OIG conducted a comparison of USIBWC documented controls agency-wide with Federal requirements outlined in the Office of Management and Budget (OMB) Memorandum M-07-16 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, Appendix J, "Privacy Control Catalog." The results are presented in Table E.1.

(U) Table E.1: Comparison of Personally Identifiable Information Policies to Federal Requirements

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
1. (U) Review and reduce the volume of PII	(U) Agencies must review current holdings of all PII and reduce to the minimum necessary	OMB M-07-16	Yes
2. (U) Reduce the use of Social Security numbers	a. (U) Agencies must review the use of Social Security numbers in agency systems and programs to identify instances in which collection or use of the Social Security numbers is superfluous	OMB M-07-16	a. Yes
	b. (U) Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security numbers		b. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
3. (U) Encryption	(U) Agencies must encrypt using only NIST certified cryptographic modules all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive in writing by the Deputy Secretary or a senior-level individual	OMB M-07-16	Yes
4. (U) Control Remote Access	(U) Agencies must allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access	OMB M-07-16	Yes
5. (U) Time-Out Function	(U) Agencies must use a time-out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity	OMB M-07-16	Yes
6. (U) Log and Verify	(U) Agencies must log all computer-readable data extracts from databases holding sensitive information and verify each extract	OMB M-07-16	Not applicable
7. (U) Ensure understanding of responsibilities	(U) Agencies must ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities	OMB M-07-16	Yes
8. (U) Authority to collect (AP-1)	(U) Agencies must determine and document the legal authority that permits the collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system need	NIST SP 800-53, rev. 4, Appendix J	No
9. (U) Purpose specification (AP-2)	(U) Agencies must describe the purpose for which PII is collected, used, maintained, and shared in its privacy notices	NIST SP 800-53, rev. 4, Appendix J	Yes
10. (U) Governance and privacy program (AR-1)	a. (U) Agencies must appoint a Senior Agency Official for Privacy/Chief Privacy Officer accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing,	NIST SP 800-53, rev. 4, Appendix J	a. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
	and disposal of PII by programs and information systems		
	b. (U) Agencies must monitor Federal privacy laws and policy for changes that affect the privacy program		b. Yes
	c. (U) Agencies must allocate sufficient resources to implement and operate the organization-wide privacy program		c. Yes
	d. (U) Agencies must develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures		d. Yes
	e. (U) Agencies must develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII		e. Yes
	f. (U) Agencies must update privacy plan, policies, and procedures at least biennially		f. Yes
11. (U) Privacy Impact and Risk Assessment (AR-2)	a. (U) Agencies must document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must conduct Privacy Impact Assessments for information systems, programs, or other activities that pose a privacy risk		b. Yes
12. (U) Privacy requirements for contractors and service providers (AR-3)	a. (U) Agencies must establish privacy roles, responsibilities, and access requirements for contractors and service providers	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must include privacy requirements in contracts and other acquisition-related documents		b. Yes
13. (U) Privacy monitoring (AR-4)	(U) Agencies must monitor and audit privacy controls and internal privacy policy to ensure effective implementation	NIST SP 800-53, rev. 4, Appendix J	Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
14. **(U)** Privacy awareness and training (AR-5)	a. **(U)** Agencies must develop, implement, and update a comprehensive training and awareness strategy	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. **(U)** Agencies must administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or activities involving PII at least annually		b. Yes
	c. **(U)** Agencies must ensure that personnel certify acceptance of responsibilities for privacy requirements at least annually		c. Yes
15. **(U)** Privacy reporting (AR-6)	**(U)** Agencies must develop, disseminate, and update reports to the Office of Management and Budget, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates and to senior management	NIST SP 800-53, rev. 4, Appendix J	Yes
16. **(U)** Privacy-enhanced system design and development (AR-7)	**(U)** Agencies must design information systems to support privacy by automating privacy controls	NIST SP 800-53, rev. 4, Appendix J	Not applicable
17. **(U)** Accounting of disclosures (AR-8)	a. **(U)** Agencies must keep an accurate accounting of disclosures of information held in each system of records under its control	NIST SP 800-53, rev. 4, Appendix J	a. Not applicable
	b. **(U)** Agencies must retain the accounting of disclosures for the life of the record or 5 years after the disclosure is made, whichever is longer		b. Not applicable
	c. **(U)** Agencies must make the accounting of disclosures available to the person named in the record upon request		c. Not applicable
18. **(U)** Data Quality (DI-1)	a. **(U)** Agencies must confirm to the greatest extent practicable upon collection or creation of PII the accuracy, relevance, timeliness, and completeness of that information	NIST SP 800-53, rev. 4, Appendix J	a. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
	b. (U) Agencies must collect PII directly from the individual to the greatest extent practicable		b. Yes
	c. (U) Agencies must check for and correct, as necessary, any inaccurate or outdated PII used by its program or systems		c. Yes
	d. (U) Agencies must issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information		d. Yes
19. (U) Data Integrity and Data Integrity Board (DI-2)	a. (U) Agencies must document processes to ensure the integrity of PII through existing security controls	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must establish a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act		b. Not applicable
20. (U) Minimization of PII (DM-1)	a. (U) Agencies must identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent		b. Yes
	c. (U) Agencies must conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings at least annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose		c. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
21. (U) Data retention and disposal (DM-2)	a. (U) Agencies retain each collection of PII for an agency-defined time period to fulfill the purpose identified in the notice or as required by law	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access		b. Yes
	c. (U) Agencies must use agency-defined techniques or methods to ensure secure deletion or destruction of PII		c. Yes
22. (U) Minimization of PII Used in Testing, Training, and Research (DM-3)	a. (U) Agencies must develop policies and procedures that minimize the use of PII for testing, training, and research	NIST SP 800-53, rev. 4, Appendix J	a. Not applicable
	b. (U) Agencies implement controls to protect PII used for testing, training, and research		b. Not applicable
23. (U) Consent (IP-1)	a. (U) Agencies must provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII		b. Yes
	c. (U) Agencies must obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII		c. Yes
	d. (U) Agencies must ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that		d. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
	was in effect at the time the organization collected the PII		
24. (U) Individual Access (IP-2)	a. (U) Agencies must provide individuals the ability to have access to their PII maintained in its system(s) of records	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records		b. Yes
	c. (U) Agencies must publish access procedures in System of Records Notices		c. Yes
	d. (U) Agencies must adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests		d. Yes
25. (U) Redress (IP-3)	a. (U) Agencies must provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended		b. Yes
26. (U) Complaint Management (IP-4)	(U) Agencies must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices	NIST SP 800-53, rev. 4, Appendix J	Yes
27. (U) Inventory of PII (SE-1)	a. (U) Agencies must establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. (U) Agencies must provide each update of the PII inventory to the Chief Information Officer or information security official to support the establishment of information security requirements for all		b. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
	new or modified information systems containing PII		
28. **(U)** Privacy Incident Response (SE-2)	a. **(U)** Agencies must develop and implement a Privacy Incident Response Plan	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. **(U)** Agencies must provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan		b. Yes
29. **(U)** Privacy Notice (TR-1)	a. **(U)** Agencies must provide effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary	NIST SP 800-53, rev. 4, Appendix J	a. No
	b. **(U)** Agencies must describe: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected		b. Yes
	c. **(U)** Agencies must revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change		c. Yes
30. **(U)** System of Records	a. **(U)** Agencies must publish System of Records Notices in the Federal Register,	NIST SP 800-53, rev. 4,	a. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
Notices and Privacy Act Statements (TR-2)	subject to required oversight processes, for systems containing PII	Appendix J	
	b. **(U)** Agencies must keep System of Records Notices current		b. No
	c. **(U)** Agencies must include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected		c. Yes
31. **(U)** Dissemination of Privacy Program Information (TR-3)	a. **(U)** Agencies must ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy/Chief Privacy Officer	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. **(U)** Agencies must ensure that its privacy practices are publicly available through organizational websites or otherwise		b. Yes
32. **(U)** Internal Use (UL-1)	**(U)** Agencies must use PII internally only for the authorized purpose identified in the Privacy Act and/or in public notices	NIST SP 800-53, rev. 4, Appendix J	Yes
33. **(U)** Information Sharing with Third parties (UL-2)	a. **(U)** Agencies must share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes	NIST SP 800-53, rev. 4, Appendix J	a. Yes
	b. **(U)** Agencies must, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used		b. Yes
	c. **(U)** Agencies must monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the		c. Yes

(U) Control	(U) Description	(U) Requirement	(U) Agency Level
	consequences of unauthorized use or sharing of PII		
	d. (U) Agencies must valuate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required		d. Yes

(U) **Source:** Office of Inspector General prepared based on documentation provided by USIBWC.

(U) *Logical Access Control Practices*

(U) USIBWC uses Active Directory to manage users' logical access at the agency level. Active Directory is a directory service created by Microsoft for Windows domain networks. It provides a capability for USIBWC to centrally manage network groups, users, computers (servers and workstations), printers, network shares, and system information, while enforcing information security standards and standardizing network configuration across the agency.

(U) USIBWC network users' authorizations are reviewed quarterly to ensure individuals who no longer require access to the network are disabled from the database of authorized users. Disabled accounts will stay in the database for 1 year before being permanently deleted. A backup of a user's email is taken prior to permanently deleting an account.

(U) USIBWC official policies and procedures (also known as directives) established Personal Identification Verification (PIV) cards per Homeland Security Presidential Directive 12 (HSPD-12) requiring agencies to issue PIV cards to Federal employees and contractors. Background checks are mandatory for a Federal employee to be issued a PIV card. These PIV cards are administered by the USIBWC's Safety and Security Division. The Safety and Security Division is responsible for issuing, re-issuing, disabling, and terminating PIV cards. PIV cards are certificate and PIN-based cards that are "personalized" with data used to grant access to Federal facilities and information systems. The issuance of PIV cards establishes the minimum dual-authentication requirement for logical or physical access to the GSS system. HSPD-12 PIV Cards are used on USIBWC workstations to access network resources.

(U) Section B. Logical Access Controls for Privileged Users and Multi-Factor Authentication for Privileged Users

(U) *The Act requires the Inspector General to provide a description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.*

(U) USIBWC privileged user accounts include Active Directory domain, server, and workstation administrator accounts. An USIBWC official stated that logical access controls are implemented

for privileged user accounts, including having the information security systems manager review privileged user accounts' activities (for example, logs captured at the Active Directory level).

(U) OIG reviewed USIBWC's policies, procedures, and practices for access controls at the agency-wide level for privileged users of information systems with PII, including a comparison of those controls with NIST standards. Table E.2 presents the results of the review.

(U) Table E.2: Comparison of Access Controls Entity-wide to Access Controls Required by Standards

(U) National Institute of Standards and Technology, Special Publication 800-53, rev. 4, Control	(U) USIBWC Policies, Procedures, and Practices at the Agency Level
(U) PL-4 Rules of Behavior Agencies establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage	(U) USIBWC requires a Rules of Behavior document be read, initialed, and signed by every employee prior to being allowed access to USIBWC systems.
(U) AC-2 Account Management • Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes for each account • Reviews accounts for compliance with account management requirements	(U) USIBWC employs the concept of least privilege, allowing only authorized access for users that are necessary to accomplish assigned tasks in accordance with each employee's position/role and business functions. Read and write rights to the assigned folders are standard permissions for non-administrative USIBWC employees. Full access is allowed Information Management Division administrators to view or change folder attributes permissions and allow formally requested mapping of data shares to other work group directories. USIBWC Form 603 "Information Technology (IT) Access Request" is required to be filled out and submitted through the work group supervisor that is being requested to be accessed and the requester to the Information Management Division for authorization and the mapping to occur. Information Management Division will concur with the work group supervisor and document the level of access provided by the requester.
(U) AC-17 Remote Access • The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed	(U) USIBWC details in the Access Control policy, usage restrictions and hardware/software required to establish remote connections to its GSS.

(U) National Institute of Standards and Technology, Special Publication 800-53, rev. 4, Control	(U) USIBWC Policies, Procedures, and Practices at the Agency Level
• The organization authorizes remote access to the information system prior to allowing such connections	(U) USIBWC requires authorization prior to configuring each user's ability to access the GSS remotely.
(U) AC-6 Least Privilege: The organization employs the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions	(U) USIBWC establishes this concept in policy and practices when applying or configuring access rights to its user community.
(U) IA-2 Identification and Authentication (Organizational Users): The information system uniquely identifies and authenticates organizational users	(U) USIBWC uses Personal Identity Verification (PIV) cards for privileged and non-privileged users and creates unique user accounts for each employee.

(U) **Source:** Office of Inspector General prepared based on documentation provided by USIBWC.

(U) USIBWC used PIV multi-authentication to govern privileged user access. If the access is from the internet, USIBWC allows users to access the network through SonicWall Virtual Private Network settings, which were in compliance with government guidelines. Also, continuous monitoring is performed by a third-party vendor, as a managed service, and is configured with one privileged account that is managed, controlled, and protected by the vendor for system administration and maintenance purposes.

(U) Section C. Reasons for Not Having Minimum Logical Access Controls and Multi-Factor Authentication for Privileged Users

(U) *If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, the Act requires the Inspector General to provide a description of the reasons for not using such logical access controls or multi-factor authentication.*

(U) USIBWC requires logical access controls or multi-factor authentication to access its covered systems.

(U) Section D. Other Information Security Management Practices

(U) *The Act requires the Inspector General to provide a description of the following information security management practices used by the covered agency regarding covered systems:*

i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

ii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –

I. data loss prevention capabilities;

II. *forensics and visibility capabilities; or*
III. *digital rights management capabilities.*

iii. *A description of how the covered agency is using the capabilities described in clause (ii).*

iv. *If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.*

(U) Software Inventory and Licenses

(U) USIBWC established and maintains an inventory of Major[7] or Minor Applications for the purpose of providing information security for the information and information systems that support operations.

(U) Monitoring and Detection of Data Exfiltration and Other Threats (Data Loss Prevention, Forensics and Visibility, and Digital Rights Management)

(U) USIBWC officials acknowledged that USIBWC did not implement data loss prevention or digital rights management solutions at the agency level for its GSS.

(U) Management's Reasons for Not Fully Implementing Data Exfiltration Controls

(U) USIBWC officials stated that the reason they did not have digital rights management technology is because it is not currently required. According to USIBWC officials, USIBWC is working with vendors to identify data loss prevention and digital rights management solutions.

(U) Section E. Entities That Provide Services to the International Boundary and Water Commission, United States and Mexico, U.S. Section

(U) *The Act requires the Inspector General to provide a description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph 4* [section D, above].

(U) USIBWC entered into an agreement with the Department of the Interior Business Center, which offers payroll, attendance, retirement, and leave management services. Access to records covered by the Business Center is permitted only to authorized personnel in accordance with requirements found in the Department of the Interior Privacy Act regulations (43 CFR 2.51). Electronic records are maintained with safeguards meeting the security requirements of 43 CFR 2.51 for automated records, which conform to OMB and Department of the Interior guidelines. Electronic data is protected through user identification, passwords, database permissions, encryption, and software controls. Security measures are established by the Business Center at

[7] **(U)** According to OMB Circular A-130, "Management of Federal Information Resources," major applications are "applications that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."

different degrees of access for different types of users. An audit trail is maintained and reviewed periodically by the Business Center. The Business Center completed a Privacy Impact Assessment, which it updates annually.

(U) ABBREVIATIONS

CONOPS Concept of Operations

DHS Department of Homeland Security

FISMA Federal Information Security Management Act of 2002

GSS General Support System

ISCM Information Security Continuous Monitoring

Modernization Act The Federal Information Security Modernization Act of 2014

NIST National Institute of Standards and Technology

OIG Office of Inspector General

OMB Office of Management and Budget

PII personally identifiable information

PIV Personal Identification Verification

SBIWTP South Bay International Wastewater Treatment Plant

SCADA Supervisory Control and Data Acquisitions

SP Special Publication

US-CERT United States Computer Emergency Readiness Team

USIBWC International Boundary and Water Commission, United States and Mexico, U.S. Section

(U) OIG AUDIT TEAM MEMBERS

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Steve Matthews, Audit Manager
Information Technology Division
Office of Audits

James DeLoach, 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