

**International Boundary and Water Commission
South Bay International Wastewater Treatment Plant
(SBIWTP) Supervisory Control and Data Acquisition
(SCADA) System
System Security Plan**



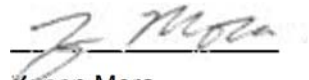
Submitted to
The Information Management Division,
U.S. Section
El Paso, TX 79902

Version Control

Date	Author	Version
09/013/2016	Corey Lancaster	1.0 – Initial Draft
09/22/2016	R. Smith	Updated diagram.
10/15/18	WachField Industries	Updated Controlls
04/10/20	Z. Mora	2.0 Updated

1 SIGNATURES AND APPROVAL

I have read and understand the security controls that are defined in this document. The signature below signifies an approval for the SBIWTP SCADA System (System) to remain in operation.



Zenon Mora
Supervisory, IT Specialist / ISSM

4/10/20

Date

Table of Contents

1	SIGNATURES AND APPROVAL	ii
1	SYSTEM CHARACTERIZATION	1
1.1	System Name and Unique Project Identifier	1
1.2	System Type	1
1.3	System Categorization.....	1
1.4	System Status.....	1
1.5	Responsible Organization.....	1
1.6	Information Contacts.....	1
1.7	General Description / Purpose.....	1
1.8	System Environment.....	2
1.9	System Interconnection / Information Sharing	3
1.9.1	System Dependencies.....	3
1.9.2	System Component Inventory	3
1.10	Applicable Laws or Regulations Affecting the System	5
1.11	FIPS 199 Levels	6
1.11.1	Security Categorization/Information Type(s)	7
1.11.2	Protection Requirements	9
1.11.3	Protection Requirement Findings	9
2	MANAGEMENT CONTROLS.....	10
2.1	(CA) Security Assessment and Authorization	10
2.1.1	(CA-1) Security Assessment and Authorization Policies and Procedures ...	10
2.1.2	(CA-2) Security Assessments.....	10
2.1.3	(CA-3) Information System Connections	11
2.1.4	(CA-5) Plan of Action and Milestones.....	12
2.1.5	(CA-6) Security Authorization	12
2.1.6	(CA-7) Continuous Monitoring	12
2.2	(PL) Planning	13
2.2.1	(PL-1) Security Planning Policy and Procedures.....	13
2.2.2	(PL-2) System Security Plan	14
2.2.3	(PL-4) Rules of Behavior	15

2.2.4	(PL-8) Information Security Architecture.....	15
2.3	(RA) Risk Assessment.....	16
2.3.1	(RA-1) Risk Assessment Policy and Procedures.....	16
2.3.2	(RA-2) Security Categorization.....	16
2.3.3	(RA-3) Risk Assessment	17
2.3.4	(RA-5) Vulnerability Scanning	17
2.4	(SA) System and Services Acquisition.....	19
2.4.1	(SA-1) System and Services Acquisition Policy and Procedures	19
2.4.2	(SA-2) Allocation of Resources	19
2.4.3	(SA-3) Life Cycle Support.....	20
2.4.4	(SA-4) Acquisitions.....	21
2.4.5	(SA-5) Information System Documentation	22
2.4.6	(SA-8) Security Engineering Principles.....	23
2.4.7	(SA-9) External Information System Services	23
2.4.8	(SA-10) Developer Configuration Management.....	24
2.4.9	(SA-11) Developer Security Testing	25
2.4.10	(SA-12) Supply Chain Protection.....	25
2.4.11	(SA-15) Development Process, Standards, and Tools	25
2.4.12	(SA-16) Developer Provided Training.....	26
2.4.13	(SA-17) Developer Security Architecture and Design.....	26
3	OPERATIONAL CONTROLS.....	26
3.1	(AT) Awareness and Training	26
3.1.1	(AT-1) Security Awareness and Training Policy and Procedures	26
3.1.2	(AT-2) Security Awareness.....	27
3.1.3	(AT-3) Role-Based Security Training.....	27
3.1.4	(AT-4) Security Training Records	28
3.2	(CM) Configuration Management.....	28
3.2.1	(CM-1) Configuration Management Policy and Procedures	28
3.2.2	(CM-2) Baseline Configuration	29
3.2.3	(CM-3) Configuration Change Control	30
3.2.4	(CM-4) Monitoring Configuration Changes	31
3.2.5	(CM-5) Access Restrictions for Change	31

3.2.6	(CM-6) Configuration Settings	32
3.2.7	(CM-7) Least Functionality	33
3.2.8	(CM-8) Information System Component Inventory	34
3.2.9	(CM-9) Configuration Management Plan	35
3.2.10	(CM-10) Software Usage Restrictions	36
3.2.11	(CM-11) User Installed Software	36
3.3	(CP) Contingency Planning.....	36
3.3.1	(CP-1) Contingency Planning Policy and Procedures	36
3.3.2	(CP-2) Contingency Plan	37
3.3.3	(CP-3) Contingency Training	39
3.3.4	(CP-4) Contingency Plan Testing	39
3.3.5	(CP-6) Alternate Storage Site	40
3.3.6	(CP-7) Alternate Processing Site.....	Error! Bookmark not defined.
3.3.7	(CP-8) Telecommunications Services	Error! Bookmark not defined.
3.3.8	(CP-9) Information System Backup	43
3.3.9	(CP-10) Information System Recovery and Reconstitution	44
3.4	(IR) Incident Response	44
3.4.1	(IR-1) Incident Response Policy and Procedures	44
3.4.2	(IR-2) Incident Response Training.....	45
3.4.3	(IR-3) Incident Response Testing and Exercises	45
3.4.4	(IR-4) Incident Handling.....	46
3.4.5	(IR-5) Incident Monitoring	46
3.4.6	(IR-6) Incident Reporting	47
3.4.7	(IR-7) Incident Response Assistance	47
3.4.8	(IR-8) Incident Response Plan	47
3.5	(MA) Maintenance.....	48
3.5.1	(MA-1) System Maintenance Policy and Procedures	48
3.5.2	(MA-2) Controlled Maintenance.....	49
3.5.3	(MA-3) Maintenance Tools	50
3.5.4	(MA-4) Remote Maintenance	50
3.5.5	(MA-5) Maintenance Personnel	51
3.5.6	(MA-6) Timely Maintenance	52
3.6	(MP) Media Protection	53

3.6.1	(MP-1) Media Protection Policy and Procedures	53
3.6.2	(MP-2) Media Access	53
3.6.3	(MP-3) Media Labeling	53
3.6.4	(MP-4) Media Storage	54
3.6.5	(MP-5) Media Transport	54
3.6.6	(MP-6) Media Sanitization and Disposal.....	54
3.6.7	(MP-7) Media Use	55
3.7	(PE) Physical and Environmental Protection	56
3.7.1	(PE-1) Physical and Environmental Protection Policy and Procedures	56
3.7.2	(PE-2) Physical Access Authorizations.....	56
3.7.3	(PE-3) Physical Access Control.....	56
3.7.4	(PE-4) Access Control for Transmission Medium	57
3.7.5	(PE-5) Access Control for Output Devices	57
3.7.6	(PE-6) Monitoring Physical Access.....	57
3.7.7	(PE-8) Access Records	58
3.7.8	(PE-9) Power Equipment and Power Cabling.....	59
3.7.9	(PE-10) Emergency Shutoff.....	59
3.7.10	(PE-11) Emergency Power	59
3.7.11	(PE-12) Emergency Lighting	59
3.7.12	(PE-13) Fire Protection.....	60
3.7.13	(PE-14) Temperature and Humidity Controls	60
3.7.14	(PE-15) Water Damage Protection.....	61
3.7.15	(PE-16) Delivery & Removal.....	61
3.7.16	(PE-17) Alternate Work Site	Error! Bookmark not defined.
3.7.17	(PE-18) Location of Information System Components.....	61
3.8	(PS) Personnel Security.....	61
3.8.1	(PS-1) Personnel Security Policy and Procedures	61
3.8.2	(PS-2) Position Categorization	62
3.8.3	(PS-3) Personnel Screening.....	62
3.8.4	(PS-4) Personnel Termination	62
3.8.5	(PS-5) Personnel Transfer.....	63
3.8.6	(PS-6) Access Agreements	63
3.8.7	(PS-7) Third-Party Personnel Security	64

3.8.8	(PS-8) Personnel Sanctions	64
3.9	(SI) System and Information Integrity.....	64
3.9.1	(SI-1) System and Information Integrity Policy and Procedures	65
3.9.2	(SI-2) Flaw Remediation.....	65
3.9.3	(SI-3) Malicious Code Protection.....	66
3.9.4	(SI-4) Information System Monitoring Tools and Techniques.....	66
3.9.5	(SI-5) Security Alerts and Advisories	68
3.9.6	(SI-6) Security Functionality Verification.....	68
3.9.7	(SI-7) Software and Information Integrity.....	69
3.9.8	(SI-8) Spam Protection	70
3.9.9	(SI-10) Information Accuracy, Completeness, Validity, and Authenticity	70
3.9.10	(SI-11) Error Handling	71
3.9.11	(SI-12) Information Output Handling and Retention.....	71
3.9.12	(SI-16) Memory Protection	71
4	TECHNICAL CONTROLS	71
4.1	(AC) Access Control	71
4.1.1	(AC-1) Access Control Policy and Procedures	71
4.1.2	(AC-2) Account Management.....	72
4.1.3	(AC-3) Access Enforcement	74
4.1.4	(AC-4) Information Flow Enforcement	74
4.1.5	(AC-5) Separation of Duties	75
4.1.6	(AC-6) Least Privilege	75
4.1.7	(AC-7) Unsuccessful Login Attempts.....	76
4.1.8	(AC-8) System Use Notification.....	76
4.1.9	(AC-10) Concurrent Session Control	77
4.1.10	(AC-11) Session Lock.....	77
4.1.11	(AC-12) Session Termination	78
4.1.12	(AC-14) Permitted Actions w/o Identification or Authentication	78
4.1.13	(AC-17) Remote Access.....	78
4.1.14	(AC-18) Wireless Access Restrictions Control: The organization:.....	79
4.1.15	(AC-19) Access Control for Portable and Mobile Devices	80
4.1.16	(AC-20) Use of External Information Systems.....	80

4.1.17 (AC-21) Information Sharing.....	81
4.1.18 (AC-22) Publicly Accessible Content.....	81
4.2 (AU) Audit and Accountability	82
4.2.1 (AU-1) Audit and Accountability Policy and Procedures	82
4.2.2 (AU-2) Auditable Events	82
4.2.3 (AU-3) Content of Audit Records	83
4.2.4 (AU-4) Audit Storage Capacity	84
4.2.5 (AU-5) Response to Audit Processing Failures	84
4.2.6 (AU-6) Audit Monitoring, Analysis, and Reporting	84
4.2.7 (AU-7) Audit Reduction and Report Generation	85
4.2.8 (AU-8) Time Stamps.....	86
4.2.9 (AU-9) Protection of Audit Information.....	86
4.2.10 (AU-10) Non-Repudiation	87
4.2.11 (AU-11) Audit Record Retention	87
4.2.12 (AU-12) Audit Generation	88
4.3 (IA) Identification and Authentication	88
4.3.1 (IA-1) Identification and Authentication Policy and Procedures	88
4.3.2 (IA-2) User Identification and Authentication	89
4.3.3 (IA-3) Device Identification and Authentication.....	90
4.3.4 (IA-4) Identifier Management.....	91
4.3.5 (IA-5) Authenticator Management	91
4.3.6 (IA-6) Authenticator Feedback.....	92
4.3.7 (IA-7) Cryptographic Module Authentication.....	92
4.3.8 (IA-8) Cryptographic Module Authentication.....	93
4.4 (SC) System and Communications Protection.....	93
4.4.1 (SC-1) System and Communications Protection Policy and Procedures.....	93
4.4.2 (SC-2) Application Partitioning	94
4.4.3 (SC-3) Security Function Isolation.....	94
4.4.4 (SC-4) Information Remnants.....	94
4.4.5 (SC-5) Denial of Service Protection.....	94
4.4.6 (SC-7) Boundary Protection	95
4.4.7 (SC-8) Transmission Confidentiality and Integrity	96
4.4.8 (SC-10) Network Disconnect	97

4.4.9	(SC-12) Cryptographic Key Establishment and Management	97
4.4.10	(SC-13) Use of Cryptography	97
4.4.11	(SC-15) Collaborative Computing Control: The information system:	97
4.4.12	(SC-17) Public Key Infrastructure Certificates	98
4.4.13	(SC-19) Voice Over Internet Protocol	98
4.4.14	(SC-20) Secure Name/Address Resolution Service (Authoritative Source). 98	
4.4.15	(SC-21) Secure Name/Address Resolution Service (Recursive or Caching Resolver)	99
4.4.16	(SC-22) Architecture and Provisioning for Name/Address Resolution Service 99	
4.4.17	(SC-23) Session Authenticity.....	99
4.4.18	(SC-28) Protection of Information at Rest.....	99
4.5	(PM) Program Management	99
4.5.1	(PM-1) Program Management Policy and Procedures	99
4.5.2	(PM-2) Senior Information Security Officer	100
4.5.3	(PM-3) Information Security Resources.....	100
4.5.4	(PM-4) Plan of Action and Milestones	101
4.5.5	(PM-5) Information System Inventory	101
4.5.6	(PM-6) Information Security Measures of Performance.....	101
4.5.7	(PM-7) Enterprise Architecture	101
4.5.8	(PM-8) Critical Infrastructure Plan	102
4.5.9	(PM-9) Risk Management Strategy	102
4.5.10	(PM-10) Security Authorization Process.....	102
4.5.11	(PM-11) Mission/Business Process Definition	103
4.5.12	(PM-12) Insider Threat Program.....	103
4.5.13	(PM-13) Information Security Workforce	103
4.5.14	(PM-14) Testing, Training, and Monitoring	103
4.5.15	(PM-15) Contacts With Security Groups and Organizations.....	104
4.5.16	(PM-16) Threat Awareness Program.....	104

APPENDIX A SYSTEM STEWARD AND AO RESPONSIBILITIES ..1

1 SYSTEM CHARACTERIZATION

1.1 System Name and Unique Project Identifier

The system name is South Bay International Water Treatment Plant (SBIWTP) SCADA.

1.2 System Type

The System is a General Support System (GSS). The SCADA Network governs all processes of the wastewater treatment plant.

1.3 System Categorization

The System is categorized with a FIPS 199 Criticality Watermark of High. The Information Types that were selected are taken from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 2. The selected information types are listed in the table below with a supporting rationale for the Availability, Integrity, and Confidentiality security services in that order.

1.4 System Status

The System has completed a major modification and upgrade and is in full operation.

1.5 Responsible Organization

The organization that is responsible for the System is the International Boundary and Water Commission (IBWC).

1.6 Information Contacts¹

The following is contact information for the System points of contact System Stewards and the Authorizing Official (AO).

Table 1- 1: Point of Contact List

	Business Steward	Security Steward	Authorizing Official
Name	Nicolas Chapa	Zenon Mora	Jayne Harkins
Title	System Owner	ISSM	Commissioner
Address	2995 Clearwater Way, in San Diego, CA, 92173	4191 N. Mesa, El Paso, TX 79902	4191 N. Mesa, El Paso, TX 79902
Phone	(619) 662-7600	(915) 832-4755	(915) 832-4101
E-mail	Nicolas.Chapa@ibwc.gov>	z.mora@ibwc.gov	Jayne.Harkins@ibwc.gov

1.7 General Description / Purpose

The SBIWTP is a 25 million gallons per day advanced primary treatment plant located in San Diego County, California, about 2 miles west of the San Ysidro Port of Entry. The physical - chemical plant treats sewage

¹ System Stewards and AO responsibilities are in Appendix A.

originating in Tijuana, Mexico and discharges it to the Pacific Ocean through the South Bay Ocean Outfall, a four and one-half mile long 11foot diameter pipe completed in January 1999.

The South Bay International Wastewater Treatment Plant (SBIWTP) was designed to deal with the growing demand for the treatment of wastewater resulting in the contamination of the Tijuana River in the United States. It has been an ongoing concern since 1934 when the International Boundary Commission (IBC) was instructed by the United States and Mexican governments to cooperate in the preparation of a report on the Tijuana sewage problem. The SBIWTP is capable of providing secondary treatment for 25 million gallons per day (mgd) average daily flows of sewage in excess of the Tijuana sewage system capacity but has expansion capability of up to 100 mgd. The SBIWTP was built on a 75-acre site near the international boundary in the U.S.

The purpose of the SCADA Network is to monitor and control the industrial processes that comprise the entire wastewater treatment plant. Every industrial process has modifiers with established set-points that the processes cannot exceed (i.e. chlorine content must have certain potency levels). The SCADA Network ensures that all of the established industrial processes within the SBIWTP Industrial Control System (ICS) operate within these defined set-points.

The USIBWC is a federal government agency and is headquartered in El Paso, Texas. The IBWC operates under the foreign policy guidance of the Department of State (DoS).

1.8 System Environment

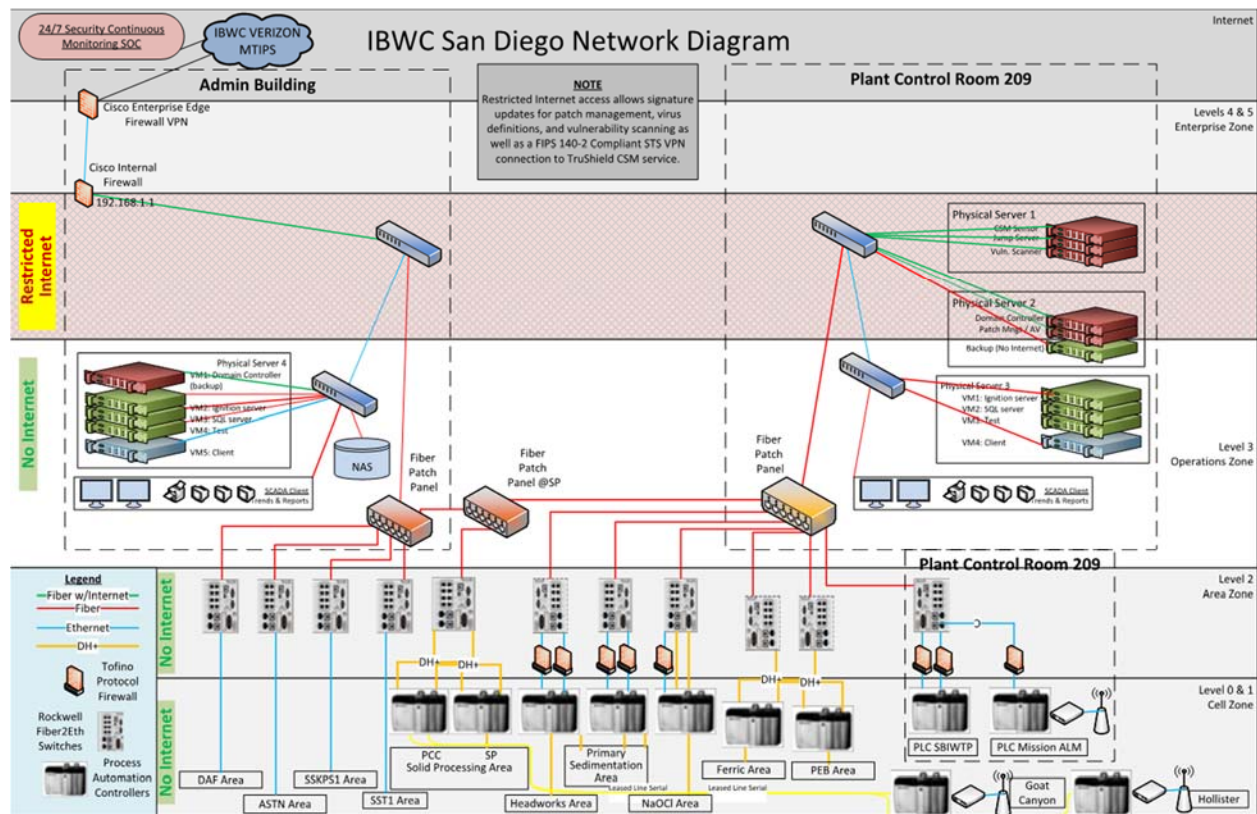


Figure 1-1: IBWC - SBIWTP Network Diagram

1.9 System Interconnection / Information Sharing

Table 1- 2: System Interconnection/Information Sharing

System Name	Responsible Organization	Type (e.g. TCP/IP)	SIA/MOU/ MOA	Date	FIPS 199 Rating (Low, Moderate, High)	ATO (Yes/No)
CDM	GovPlace	Security Monitoring	MOU	2020	High	No

1.9.1 System Dependencies

The following is a list of dependencies for the System:

- Bioreactor Mixer
- Bioreactor #1 - #3 Valve
- Bioreactor #1 - #3 Mixed Liquor
- Grit Pump #1 - #2
- Air Blower #1 - #5
- Secondary Clarifier #1 - #3
- RAS Pump #1 - #5
- WAS Valves
- WAS Pumps
- Rotary Drum Thickener #1 and #2
- Polymer System Station
- SE Pump Station #1 - #3
- WSSP Aerator #1-4
- Generator and ATS Station
- MDT Auto-save
- Alarm System

1.9.2 System Component Inventory

Below is a table of the SCADA Network Component Inventory

Table 1-3: SCADA Network Inventory

Host Name	Description	IP Address	Subnet Mask	Default Gateway	DNS	DMZ Status
ESX Host	ESX Host	192.198.2.20	255.255.255.0	192.198.0.1	192.168.20.0.10	
	IDRAC	192.168.2.23	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DC-01	Domain Controller	192.168.2.38	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DC-01	Domain Controller	192.168.1.38	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone

Host Name	Description	IP Address	Subnet Mask	Default Gateway	DNS	DMZ Status
SAND-IBWC-AP-01	SAND-IBWC-AP-01	192.168.2.39	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-AP-01	SAND-IBWC-AP-01	192.168.1.39	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-AP-02	SAND-IBWC-AP-02	192.168.2.40	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-AP-02	SAND-IBWC-AP-02	192.168.1.40	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SD-VSHERE	SD-VSHERE	192.168.2.41	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
ESX Host	ESX Host	192.198.2.21	255.255.255.0	192.198.0.1	192.168.20.0.10	Inside Zone
	IDRAC	192.168.2.24	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-IG-01	SAND-IBWC-IG-01	192.168.2.42	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DB-01	Database	192.168.2.43	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-TST-01	SAND-IBWC-TST-01	192.168.2.44	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-CT-01	SAND-IBWC-CT-01	192.168.2.45	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
ESX Host	ESX Host	192.198.2.22	255.255.255.0	192.198.0.1	192.168.20.0.10	Inside Zone
	IDRAC	192.168.2.25	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DC-02	Domain Controller	192.168.2.47	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DC-02	Domain Controller	192.168.1.47	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-DB-02	Database	192.168.2.48	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SAND-IBWC-IG-02	SAND-IBWC-IG-02	192.168.2.49	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SWITCH 1	SWITCH 1	192.168.2.100	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
SWITCH 2	SWITCH 2	192.168.2.101	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.80	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.81	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.82	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.83	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.84	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.85	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.86	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone

Host Name	Description	IP Address	Subnet Mask	Default Gateway	DNS	DMZ Status
	THIN CLIENTS	192.168.2.87	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.88	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.89	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.90	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.91	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.92	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.93	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.94	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.95	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	THIN CLIENTS	192.168.2.96	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
RESERVED ESX	ESX	192.168.2.22	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
RESERVED IDRAC	IDRAC	192.168.2.25	255.255.255.0	192.168.0.1	192.168.20.0.10	Inside Zone
	GovPlace Sensor	152.180.135.236	255.255.255.0	152.180.1.236	192.168.20.0.10	Outside Zone

1.10 Applicable Laws or Regulations Affecting the System

The U.S. IBWC is responsible for implementing and administering a security program to protect its information resources in compliance with federal laws and regulations. The following section denotes applicable laws and regulations, standards, and guidelines from which USIBWC system security requirements are derived.

Executive Orders (EO)

- EO 10450 Security Requirements for Government Employment
- EO 10310 Critical Infrastructure Protection
- EO 13011 Federal Information Technology
- EO 13103 Computer Software Piracy
- Homeland Security Presidential Directive 7

Federal Laws

- Title II of the E-Government Act of 2002, Section 208
- Privacy Act of 1974 (P.L. 93-579)
- Freedom of Information Act of 1974
- Federal Records Management Acts

- Computer Fraud and Abuse Act of 1986 (P.L. 99-474)
- Clinger-Cohen Act of 1996
- Defense Authorization Act (P.L. 106-398)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191)
- Federal Information Security Management Act of 2002 (FISMA)

National Institute of Standards and Technology (NIST) Special Publication (SP) and Guidelines

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems
- NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for IT Systems
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems
- NIST SP 800-60 Vol. 1 & 2, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-63, Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology
- NIST SP 70, The NIST Security Configuration Checklists Program
- NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-86, Guide to Integrating Forensic Techniques Into Incident Response
- NIST SP 800-92, Guide for Computer Security Log Management
- NIST SP 800-97, Guide to IEEE 802.111: Establishing Robust Security Networks (this is related to wireless network deployment)

Federal Information Processing Standards Publications (FIPS)

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems

Office of Management and Budget (OMB) Circulars and Government Accounting Office (GAO) Requirements

- OMB Circular No. A-130, Appendix III
- OMB Circular No. A-123, Management Accountability and Control
- OMB M-02-01, Guideline for Preparing and Submitting Security Plans of Action and Milestones

1.11 FIPS 199 Levels

FIPS 199 establishes three potential impact levels (Low, Moderate, High) for each of the security objectives (confidentiality, integrity, and availability). For any ICS/SCADA system, these security services are generally prioritized as availability, integrity, and confidentiality (A/I.C) in that order. The impact levels focus on the potential impact and magnitude of harm that the loss of these security services would have on

SBIWTP's operations, assets, or individuals. FIPS 199 recognizes that an information system may contain more than one type of information (e.g., privacy information, medical information, financial information), each of which is subject to security categorization.

The following table provides the definitions for the A/I/C ratings for the System.

Table 1-4: Security Objectives

Security Objective	Low	Moderate	High
<i>Availability</i> Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<i>Integrity</i> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC, SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

1.11.1 Security Categorization/Information Type(s)

The security category of an information system that processes, stores, or transmits multiple types of information should be at least the highest impact level that has been determined for each type of information for each security objective of A/I/C. The following table depicts the security category/information type for The System as identified in the System Risk Assessment Report.

Table 1- 5: System Information Types

Information Type / Rationale	NIST SP 800-60 Reference	Availability Low/Moderate/High	Integrity Low/Moderate/High	Confidentiality Low/Moderate/High
Service Recovery Service recovery involves the internal actions necessary to develop a plan for resuming operations after a catastrophe occurs, such as a fire or an earthquake. The System generates alarms of what actions must be done to restore any part of wastewater treatment	C.2.4.3	High	Moderate	Low
Water Resource Management Water Resource Management includes all activities that promote the effective use and management of the nation's water resources. The System controls all activities for wastewater treatment.	D.6.1	High	High	Low
Pollution Prevention and Control Pollution prevention and control includes activities associated with the establishment of environmental standards to control the levels of harmful substances emitted into the soil, water, and atmosphere. T	D.8.3	High	High	Low
Public Resources, Facility, and Infrastructure Management Public Resources, Facility, and Infrastructure Management involve the management and maintenance of government-owned capital goods and resources (natural or otherwise) on behalf of the public. T	D.22.3	High	High	Low
Overall Rating	High	High	High	Low

Based on the information types listed in the table provided above, the criticality watermark for the System is High.

1.11.2 Protection Requirements

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for the A/I/C of the information: Availability relates to the impact to the organization should the system be unavailable for use. Integrity ensures that the system's information remains unaltered during transit. The goal of Confidentiality is to ensure that the data can only be disclosed to those to whom the data is intended.

1.11.3 Protection Requirement Findings²

- **Confidentiality:** The System contains information that could identify information about the City's water supply. This data requires a minimal level of protection from unauthorized disclosure because it is generally made publicly available. If the certain information contained in the System were released to the public it could result in a loss of public confidence in the city's resource management. However, the consequences are evaluated as minimal. Therefore, the unauthorized disclosure of the System information could be expected to have a minimal effect on organizational operations, SBIWTP assets, or individuals and the information. The protection measures are rated as **Low**.
- **Integrity:** The System collects and processes information regarding natural resource management. Because the wastewater treatment and chemical levels depend on the accuracy of the data collected, the unauthorized and unanticipated modification could seriously impact the health of the community population at large. Therefore, the unauthorized modification of the System information could be expected to have a severe effect on SBIWTP operations, organizational assets, or individuals and the information and protection measures are rated as **High**.
- **Availability:** If the System were unavailable for even a short period of time, it would have an immediate impact and would affect the ability of the City to have access to a safe water supply. Therefore, the unavailability of the System information could be expected to have a severe effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **High**.

²Low – a limited adverse effect

Moderate – a serious adverse effect

High – a severe or catastrophic adverse effect

2 MANAGEMENT CONTROLS

2.1 (CA) Security Assessment and Authorization

2.1.1 (CA-1) Security Assessment and Authorization Policies and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
- b. Reviews and updates the current:
 1. Security assessment and authorization policy annually; and
 2. Security assessment and authorization procedures annually.

Implementation:

Inherited Control

The SBIWTP follows the IBWC Security Assessment and Authorization policies and procedures that are established for all IBWC information systems. IBWC has developed, documented and disseminated the following:

- a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among IBWC entities, and compliance with the appropriate standards for all IBWC information systems. IBWC has developed procedures to facilitate the implementation of the security authorization policy and associated controls for all IBWC-owned information systems.
- b. IBWC reviews and updates the security assessment and authorization policy annually. Security assessment and authorization procedures for all IBWC information systems are also updated annually.

2.1.2 (CA-2) Security Assessments

Control: The organization:

- a. Develops a security assessment plan that describes the scope of the assessment including:
 1. Security controls and control enhancements under assessment;
 2. Assessment procedures to be used to determine security control effectiveness; and
 3. Assessment environment, assessment team, and assessment roles and responsibilities;
- b. Assesses the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
- c. Produces a security assessment report that documents the results of the assessment; and
- d. Provides the results of the security control assessment SBITWP operations and SCADA system maintenance contractors.

Implementation:

System Specific Control

The SBIWTP has implemented the following to address security assessments:

- a. A security assessment plan that describes the scope of the assessment. The plan discusses the scope of the security controls and the security control enhancements that are involved in the assessment. The plan also details the assessment procedures that

are to be used to determine the security control effectiveness. Further, the security assessment plan also discusses the assessment environment, the assessment team, along with the assessment roles and responsibilities.

- b. Security controls are assessed annually in the SCADA Network to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the established security requirements.
- c. A security assessment report is provided that documents the results of the assessment.
- d. The results of the security control assessment are currently provided to the IBWC ISSM.

CA-2(1) *SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*

The organization employs assessors or assessment teams to conduct security control assessments.

Implementation:

System Specific Control

The SBIWTP has employed a team of assessors to conduct security control assessments. This team is employed by IBWC but is independent of IBWC operations.

CA-2(2) *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*

The organization includes as part of security control assessments, specialized, *in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing.*

Implementation:

System Specific Control

The SBIWTP has implemented the following to address specialized security assessments. The SBIWTP has deployed a Continuous Security Monitoring (CDM) solution that provides in-depth monitoring and analysis as part of its security control assessments. IBWC uses an independent team to perform quarterly vulnerability assessments of the System to include all support equipment and system.

2.1.3 (CA-3) Information System Connections

Control: The organization:

- a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
- b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
- c. Reviews and updates Interconnection Security Agreements annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address information system connections:

- a. All appropriate connections have been authorized from the SCADA Network to other information systems through the use of Interconnection Security Agreements (ISA)s
- b. The interface characteristics, security requirements, and the information communicated are documented for each defined interconnection.
- c. The ISAs are reviewed and updated annually. An ISA is currently in place with the vendor which perform the 24/7 security monitoring of the SCADA Network.

CA-3(5) *SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*

The organization employs *deny-all* policy for allowing SCADA system components to connect to external information systems.

Implementation:

System Specific Control

The SBIWTP employs a deny-all and no direct internet connects to the core layer of the SCADA system, in extreme emergencies SBIWTP may permit an exception to the policy to allow connections to the SCADA Network.

2.1.4 (CA-5) Plan of Action and Milestones

Control: The organization:

- a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Updates existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to create a Plan of Action and Milestones (POA&M):

- a. SBIWTP has developed a POA&M for the System to document the planned remedial actions to correct weaknesses and deficiencies noted during the assessment of the security controls. Known vulnerabilities are reduced and/or eliminated via the POA&M.
- b. The POA&M is updated after every security assessment or when anomalies are detected by the monitoring services. The POA&M is based on any findings from security control assessments, security impact analyses, and continuous monitoring activities.

2.1.5 (CA-6) Security Authorization

Control: The organization:

- a. Assigns a senior-level executive or manager as the authorizing official for the information system;
- b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
- c. Updates the security authorization annually

Implementation:

System Specific Control

The SBIWTP completes the following activities for security authorization of the System:

- a. The USBWC Commissioner is the senior level executive who is assigned as the authorizing official for the SCADA Network.
- b. The authorizing official always authorizes the SCADA Network before commencing operations of any system upgrades.
- c. The security authorization package is updated on an ongoing basis.

2.1.6 (CA-7) Continuous Monitoring

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

- a. Establishment of SCADA components to be monitored;
- b. Establishment of continuous monitoring assessments supporting such monitoring;
- c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
- e. Correlation and analysis of security-related information generated by assessments and monitoring;
- f. Response actions to address results of the analysis of security-related information; and

- g. Reporting the security status of the organization and the information system to SBITWP operations and SCADA maintenance contractors annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address continuous monitoring:

The SBIWTP has developed a continuous monitoring solution and has implemented a continuous monitoring program using the Continuous Diagnostics and Monitoring (CDM) Services provided by GovPlace Solutions. This solution includes the following:

- a. A clearly defined set of metrics to be monitored by the CDM service.
- b. CDM establishes a continuous frequency for assessments that support each monitoring activity.
- c. CDM supports ongoing security control assessments that occur on an annual basis in accordance with the continuous monitoring solution.
- d. CDM provides continuous security status monitoring of a set of defined metrics in accordance with the SBIWTP continuous monitoring solution.
- e. CDM provides correlation services for analysis of security-related information that is generated by security assessments and continuous monitoring activities.
- f. CDM provides response actions to address the results of the analysis of security related information.
- g. The security status of the SCADA Network and other related SBIWTP assets is provided to GovPlace Security staff and the appropriate IBWC personnel on a continuous basis.

CA-7(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

The organization employs 3rd party assessors or assessment teams to monitor the security controls in the information system on an ongoing basis.

Implementation:

System Specific Control

The SBIWTP employs the GovPlace Security Solutions CDM security staff to monitor the security controls of the SCADA Network on an ongoing basis. GovPlace Security Solutions operates independently from SBIWTP and IBWC.

2.2 (PL) Planning

2.2.1 (PL-1) Security Planning Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to IBWC personnel and CDM services providers:
 - 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
- b. Reviews and updates the current:
 - 1. Security planning policy annually; and
 - 2. Security planning procedures annually.

Implementation:

System Specific Control

SBIWTP has developed documentation for security planning policies and procedures.

- a. The security planning policy is disseminated to the System Owner and the SBIWTP ISSM. The policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy

includes and associated security planning controls necessary for implementation as well as procedures to facilitate the implementation.

- b. The security planning policy and its associated procedures are reviewed and updated annually.

2.2.2 (PL-2) System Security Plan

Control: The organization:

- a. Develops a security plan for the information system that:
 1. Is consistent with the organization's enterprise architecture;
 2. Explicitly defines the authorization boundary for the system;
 3. Describes the operational context of the information system in terms of missions and business processes; connections to other information systems;
 4. Provides the security categorization of the information system including supporting rationale;
 5. Describes the operational environment for the information system and relationships with or
 6. Provides an overview of the security requirements for the system;
 7. Identifies any relevant overlays, if applicable;
 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
 9. Is reviewed and approved by the authorizing official or designated representative prior to planning implementation;
- b. Distributes copies of the security plan and communicates subsequent changes to the plan to SBITWP operations and SCADA maintenance contractors ;
- c. Reviews the security plan for the information system annually;
- d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
- e. Protects the security plan from unauthorized disclosure and modification.

Implementation:

System Specific Control

- a. The IBWC's IMD has developed a system security plan for this SCADA System. This document serves as the SBIWTP System Security Plan (SSP). The SSP is consistent with the SBIWTP ICS architecture. It explicitly defines Layer 2 of the SBIWTP ICS as the proper security authorization boundary. It describes the operational context of the System in terms of the mission, business processes, and connections to other information systems. The security categorization information and its supporting rationale are provided in Section 1.11.1 of this document. This SSP describes the operational environment in relation to all other connected information systems. It also describes all security requirements of the System and the security controls that are in place and planned to meet these requirements, including any tailored controls with their supporting rationale. It has been reviewed by the designated approving authority prior to implementation.
- b. Copies of this SSP have been distributed to the System Owner and the ISSM.
- c. The SSP for the System is reviewed and updated annually.
- d. The SSP will be updated to address changes to the SCADA Network environment of operation. Any problems identified during implementation or during security control assessments will be documented in this SSP.
- e. This SSP is protected from unauthorized disclosure or modification by only distributing it in areas that can be accessed by authorized personnel such as protected SharePoint sites.

The organization plans and coordinates security-related activities affecting the information system with the SBIWTP operations contractor before conducting such activities in order to reduce the impact on other organizational entities.

Implementation:

System Specific Control

The SBIWTP plans and coordinates security-related activities that affect the System with the SCADA Network senior level executives. These activities are coordinated prior to executing these activities in order to reduce the impact on other entities that are related to IBWC.

2.2.3 (PL-4) Rules of Behavior

Control: The organization:

- a. Establishes and makes 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;
- b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
- c. Reviews and updates the rules of behavior bi-annually; and
- d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Implementation:

System Specific Control

The SBIWTP has created a Rules of Behavior (ROB) document that addresses the following:

- a. The ROB is made readily available to employees who require access to the System. The ROB defines rules that describe the employee's responsibilities and the expected behavior when accessing the System and its associated information.
- b. The System Owner receives a signed acknowledgment from all employees indicating that they have read, understand, and agree to abide by the ROB before access is authorized to an employee.
- c. The ROB is reviewed and updated annually at a minimum.
- d. All employees who are granted access to the SCADA Network who have signed a previous version of the ROB are required to read and re-sign the ROB when it is revised and/or updated.
- e. The ROB is also incorporated in the annual security awareness training program to ensure all employees are well versed in policy requirements.

PL-4(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Implementation:

Not Applicable

The SBIWTP does not need to include explicit restrictions on the use of social media and posting SBIWTP information on public websites because internet browsing is not enabled on the SCADA Network.

2.2.4 (PL-8) Information Security Architecture

Control: The organization:

- a. Develops an information security architecture for the information system that:
 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
3. Describes any information security assumptions about, and dependencies on, external services;
- b. Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; and
- c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Implementation:

System Specific Control

The SBIWTP has created a highly segmented network architecture that consists of four (4) segments. Segment 1 is the processing zone located throughout the plant and each zone is shielded by using a Tofino firewall to filter and limit the interaction between the various zones. Segment 2 is the System. It is segregated from zone 3 and it limits the interaction to a few ports required for updates and security definitions. The architecture is tested annually to ensure the integrity of the logical and physical separation.

The goal is to ensure the processing zones and the SCADA are fully protected from the internet while allowing administration and other supporting services to be provided by an intermediary network segment which is located in segment 3. The overall architecture is depicted in the network diagram shown in Section 1.8

2.3 (RA) Risk Assessment

2.3.1 (RA-1) Risk Assessment Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to CDM service providers and SBIWTP operations contractor:
 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
- b. Reviews and updates the current:
 1. Risk assessment policy and;
 2. Risk assessment procedures bi-annually.

Implementation:

System Specific Control

The SBIWTP has developed a risk assessment policy that addresses the following:

- a. It addresses purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP and IBWC entities. It also addresses compliance standards and follows the recommendations described in ANSI 02-01:2007. The risk assessment policy addresses Health Safety and Environmental concerns as outlined in the standard.
- b. The risk assessment policy and its associated procedures are reviewed and updated annually.

2.3.2 (RA-2) Security Categorization

Control: The organization:

- a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

- b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Implementation:

System Specific Control

The SBIWTP has implemented the following to address security categorization:

- a. The System has been categorized by using the Federal Information Processing Standard (FIPS) 199 standard. The System has criticality watermark of High. This standard has been followed in accordance with all applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- b. The System has documented the security categorization results, including the supporting rationale, in Section 1.11.1 of this SSP.
- c. The SBIWTP has ensured that the authorizing official has reviewed and approved the security categorization decision by obtaining the authorizing official's signature on this SSP.

2.3.3 (RA-3) Risk Assessment

Control: The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- b. Documents risk assessment results in risk assessment reports.;
- c. Reviews risk assessment results monthly;
- d. Disseminates risk assessment results to maintenance contractors; and
- e. Updates the risk assessment monthly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Implementation:

System Specific Control

The SBIWTP has implemented the following to address risk assessments on the SCADA Network:

- a. An assessment of risk is conducted including the likelihood and magnitude of harm from resulting the following malicious activities done to the SCADA Network:
 - o Unauthorized access
 - o Use
 - o Disclosure
 - o Disruption
 - o Modification
 - o Destruction
- b. The System risk assessment results are documented in the risk assessment report.
- c. The risk assessment results are reviewed annually.
- d. The risk assessment results are disseminated to the SCADA Network system owner and authorizing official.
- e. The risk assessment is conducted and updated annually at a minimum and whenever there is a significant change to the System or it's operating. Triggers to the risk assessment update also include the identification of new threats and system hardware changes.

2.3.4 (RA-5) Vulnerability Scanning

Control: The organization:

- a. Scans for vulnerabilities in the information system and hosted applications monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - 1. Enumerating platforms, software flaws, and improper configurations;
 - 2. Formatting checklists and test procedures; and
 - 3. Measuring vulnerability impact;
- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and
- e. Shares information obtained from the vulnerability scanning process and security control assessments with SBIWTP operations contractor and SCADA maintenance contractor to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Implementation:

System Specific Control

The SBIWTP has implemented the following to address vulnerability scanning:

- a. Vulnerability scans are run in the System and all of its hosted applications monthly. Vulnerability scans are also run whenever any new vulnerability has been identified and reported.
- b. Vulnerability scanning tools and techniques are employed to facilitate interoperability among tools. The vulnerability management scans are automated as part of the GovPlace Vulnerability Management as a Service (VMaaS) process. Standards are used for enumerating platforms of the SCADA devices. Software flaws and improper configurations are also regularly monitored and detected as part of the GovPlace CDM process. The scanning tools that are employed automatically format a checklist and measure vulnerability impact.
- c. Vulnerability scan results and reports are analyzed in support of security control assessments and the established POA&M process,
- d. Legitimate vulnerabilities that are identified with a High impact are mitigated within thirty (30) calendar days from the date of discovery. Vulnerabilities that are identified with a Medium impact are mitigated within sixty (60) calendar days from the date of initial discovery. Legitimate vulnerabilities that are identified with a Low impact are mitigated within ninety (90) days of the date of initial discovery. If these vulnerabilities cannot be remediated within these timeframes a POA&M item is created with proper supporting rationale and the initial timeframes identified.
- e. The information obtained from the vulnerability scanning process and security control assessments is shared with the System Owner and the ISSM to help mitigate similar vulnerabilities in other information systems.

RA-5(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Implementation:

System Specific Control

The SBIWTP employs vulnerability scanning tools that include the capability to readily update the System vulnerabilities that will be scanned by following the GovPlace VMaaS process.

RA-5(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

The organization updates the information system vulnerabilities scanned monthly; prior to a new scan; when new vulnerabilities are identified and reported].

Implementation:

System Specific Control

The SBIWTP relies upon the VMaaS process from GovPlace to update the SCADA Network system vulnerabilities. The system vulnerabilities are updated in real-time and the signatures are immediately applied when they are identified and reported.

RA-5(4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION

The organization determines what information about the information system is discoverable by adversaries and subsequently takes corrective actions.

Implementation:

System Specific Control

The GovPlace VMaaS process provides the ISSM with monthly Security Assessment Report highlighting what information about the System is discoverable and exploitable by adversaries. The system owner is notified whenever a significant exploit is discovered. Possible options to mitigate the effects of any exploit are recommended to the system owner for review and approval.

RA-5(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

The information system implements privileged access authorization to SBIWTP maintenance contractors for selected remediation and corrective actions.

Implementation:

System Specific Control

The SBIWTP implements privileged access authorization to the VMaaS scanning server. Only GovPlace Security Operations Center (SOC) may conduct vulnerability scanning activities.

2.4 (SA) System and Services Acquisition

2.4.1 (SA-1) System and Services Acquisition Policy and Procedures

Control: The organization:

- a. Develops, and documents:
 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
- b. Reviews and updates the current:
 1. System and services acquisition policy; and
 2. System and services acquisition procedures bi-annually.

Implementation:

Inherited Control

The SBIWTP relies upon IBWC, the chief organization, to develop a system services and acquisition policy that addresses the following:

- a. The purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP and IBWC entities. It must also address compliance standards and follows the recommendations described in ANSI 02-01:2007.
- b. The system services and acquisition policy and its associated procedures are reviewed and updated annually.

2.4.2 (SA-2) Allocation of Resources

Control: The organization:

- a. Determines information security requirements for the information system or information system service in mission/business process planning;
- b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
- c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Implementation:

Hybrid Control

The SBIWTP implements the following to address the allocation of resources for the System:

- a. SBIWTP determines the information security requirements for the System in business process planning. These requirements are forwarded to IBWC for consideration and approval.
- b. SBIWTP determines and documents the amount of resources required to protect the System as part of the Capital Planning and Investment Control (CPIC) process. IBWC gives the final approval for the allocation of resources.
- c. A discrete line item for information security is recommended by SBIWTP to include in the IBWC programming and budgeting documentation.

2.4.3 (SA-3) Life Cycle Support

Control: The organization:

- a. Manages the information system using established system development life cycles that incorporates information security considerations;
- b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
- c. Identifies individuals having information security roles and responsibilities; and
- d. Integrates the organizational information security risk management process into system development life cycle activities.

Implementation:

System Specific Control

The SBIWTP implements the following to address life cycle support:

- a. SBIWTP manages the System using a System Development Lifecycle (SDLC) methodology that includes the following security framework:

SCADA Security Framework					
Administrative Controls	SCADA Controls	Data and Application Security	System Assurance	Monitoring Controls	External Controls
Organizational Leadership and Security Organization	Asset Management	Data Security	System Resilience	Incident Management	Vendor Security Management
NIST Guidance, implementation, and acceptance	Identity and Access Management	Application Security, development, and maintenance	Secure configuration	CDM	Virtual Private Networks

Risk Assessments	Vulnerability Management	Change management	Business Continuity and Disaster Recovery Planning	Forensics	
Security Awareness and Training	SCADA Network Security Controls	Malicious Code Detection/Prevention			
Concept of Operations	Physical Security				

- b. The information security roles and responsibilities have been defined throughout the established SDLC.
- c. Individuals that have information security roles have been identified and documented. The roles that have been identified are:
 - i. USIBWC ISSM – security manager
 - ii. GovPlace CDM – Security Operations Staff
- d. The SBIWTP risk management process has been incorporated into the SDLC related activities.

2.4.4 (SA-4) Acquisitions

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

- a. Security functional requirements;
- b. Security strength requirements;
- c. Security assurance requirements;
- d. Security-related documentation requirements;
- e. Requirements for protecting security-related documentation;
- f. Description of the information system development environment and the environment in which the system is intended to operate; and
- g. Acceptance criteria.

Implementation:

Hybrid Control

The SBIWTP implements the following to address system acquisitions:

- a. Security functional requirements are recommended by SBIWTP to be incorporated into the IBWC acquisition contracts.
- b. Security strength requirements are recommended by SBIWTP to be incorporated into the IBWC acquisition contracts.
- c. Security assurance requirements are recommended by SBIWTP to be incorporated into the IBWC acquisition contracts.
- d. Security related documentation requirements are included by SBIWTP to be incorporated into the IBWC acquisition contracts.
- e. Requirements for protecting security related documentation recommended by SBIWTP to be incorporated into the IBWC acquisition contracts.
- f. A description of the System environment is provided by SBIWTP to be incorporated into the IBWC acquisition contracts.

- g. Acceptance criteria are provided by SBIWTP to be incorporated into the IBWC acquisition contracts.

IBWC approves all acquisition contracts to support the System

SA-4(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address the functional properties of security controls. SBIWTP requires the developer of the System to provide a description of the functional properties of the information security controls to be employed within the System.

SA-4(2) ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; source code or hardware schematics.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address the design and implementation of security controls during the acquisition process. The SBIWTP requires the developer of the System to provide a high-level design and implementation of the security controls to be employed within the System.

SA-4(9) ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address the functions, ports, protocols, and services in use during the acquisition process. SBIWTP requires the developer of the System to identify the functions, ports, protocols, and services intended for use within the System. This is always done early in the SDLC.

SA-4(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address the use of PIV products. The SBIWTP only employs information technology products that are on the FIPS-201 approved products list for the PIV capability within the System.

2.4.5 (SA-5) Information System Documentation

Control: The organization:

- a. Obtains administrator documentation for the information system, system component, or information system service that describes:
 1. Secure configuration, installation, and operation of the system, component, or service;
 2. Effective use and maintenance of security functions/mechanisms; and
 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
- b. Obtains user documentation for the information system, system component, or information system service that describes:
 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
 3. User responsibilities in maintaining the security of the system, component, or service;
- c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes corrective actions in response;
- d. Protects documentation as required, in accordance with the risk management strategy; and
- e. Distributes documentation to SBIWTP operations and maintenance contractor.

Implementation:

System Specific Control

The SBIWTP has implemented the following to address information security documentation and its protection.

- a. Administrator documentation is obtained for the System and its components. It addresses secure configuration, installation, and operation of the System. Effective use and maintenance of the security functions designed within the System are also addressed. Known configuration vulnerabilities are also addressed within this documentation.
- b. User documentation for the System has been obtained. This documentation describes all user-accessible security functions that are applicable along with the suggested methods for effective use of these functions. Any specific user interaction that enables the system to be used in a more secure manner is also discussed where applicable. User responsibilities for effectively maintaining the security of the SCADA Network are also discussed.
- c. Attempts to obtain the System documentation when specific types of documentation are either available or non-existent.
- d. All documentation is protected in accordance with the SBIWTP risk-management strategy.
- e. The SBIWTP security documentation is distributed to the System Owner and the ISSM.

2.4.6 (SA-8) Security Engineering Principles

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Implementation:

System Specific Control

The SBIWTP applies information security engineering principles in the specification, design, development, implementation, and modification of the System.

2.4.7 (SA-9) External Information System Services

Control: The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ NIST 800-53 controls in accordance with

applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. Employs CDM services and SCADA system maintenance contractors to monitor security control compliance by external service providers on an ongoing basis.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address external information services.

- a. Providers of services that are external to the System are required to comply with the System information security policies and the specifications outlined for each of the defined security controls in accordance with all applicable federal laws, executive orders, directives, policies, standards, and guidance.
- b. Government oversight, along with user roles and responsibilities is defined with regard to external information services within the appropriate ISA.
- c. Security control assessments are employed within SBIWTP to monitor compliance with external service providers on an ongoing basis.

SA-9(2) EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

The organization requires providers of CMD service providers to identify the functions, ports, protocols, and other services required for the use of such services.

Implementation:

System Specific Control

The SBIWTP requires that all external information system service providers identify the relevant ports, protocols, and other services that must be enabled in order to use these external services.

2.4.8 (SA-10) Developer Configuration Management

Control: The organization requires the developer of the information system, system component, or information system service to:

- a. Perform configuration management during system, component, or service *development, implementation and operation*;
- b. Document, manage, and control the integrity of changes to *configuration management templates*;
- c. Implement only organization-approved changes to the system, component, or service;
- d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
- e. Track security flaws and flaw resolution within the system, component, or service and report findings to the IMD.

Implementation:

System Specific Control

The SBIWTP has taken the following additional actions to address developer configuration management.

- a. The developer is required to perform configuration management during the System design, development, and implementation.
- b. The developer must document, manage, and control the integrity of changes to the System components as defined under the configuration management process
- c. The developer is required to implement only the approved changes to the System.
- d. All approved changes to the System are required to be documented along with the potential security impacts of the changes.
- e. The developer is required to track any security flaws and the flaw remediation process within the System.

2.4.9 (SA-11) Developer Security Testing

Control: The organization requires the developer of the information system, system component, or information system service to:

- a. Create and implement a security assessment plan;
- b. Perform system testing/evaluation;
- c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- d. Implement a verifiable flaw remediation process; and
- e. Correct flaws identified during security testing/evaluation.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address developer security testing:

- a. The developer of the System is required to create and implement a security assessment plan.
- b. The developer is required to perform integration testing and evaluation upon the installation of the SCADA Network components.
- c. The developer is required to produce evidence of the execution of the security assessment plan and document the results of the testing.
- d. The developer is required to implement a verifiable flaw remediation process.
- e. The developer is required to correct flaws during the security testing and evaluation.

2.4.10 (SA-12) Supply Chain Protection

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing a comprehensive, defense-in-breadth information security strategy.

Implementation:

System Specific Control

The SBIWTP protects against threats to the supply chain of the System components by only purchasing components from an approved vendor list.

2.4.11 (SA-15) Development Process, Standards, and Tools

Control: The organization:

- a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
 1. Explicitly addresses security requirements;
 2. Identifies the standards and tools used in the development process;
 3. Documents the specific tool options and tool configurations used in the development process; and
 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- b. Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security control requirements.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address the development process, standards, and tools:

- a. The developer of the System follows a documented development process that explicitly addresses security requirements. The standards and tools are also identified in the development process. The specific tool options and configurations are also documented in supporting documentation of the development process. The integrity of any changes

to the process and the tools used in development are documented and managed appropriately.

- b. The development process, standards used, tools used, and the tool configuration options are reviewed annually to determine if these processes and tools can meet the System security requirements that are defined by policy.

2.4.12 (SA-16) Developer Provided Training

Control: The organization requires the developer of the information system, system component, or information system service to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Implementation:

System Specific Control

The SBIWTP requires the developer of the System to provide basic security training that instructs users on the correct use and the operation of the implemented security functions on the Human Machine Interfaces (HMI)s. Specific training is provided on site.

2.4.13 (SA-17) Developer Security Architecture and Design

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

- a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
- b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address developer security architecture and design:

- a. The design and specification of the System security architecture are consistent and supportive of SBIWTP's security architecture that is established. It is consistent with SBIWTP's entire ICS enterprise architecture.
- b. The required security functionality is accurately and completely described and the allocation of security controls is appropriately distributed among the physical and logical components.
- c. The individual security functions, mechanisms, and services are expressed in terms of how they work together to provide the required security capabilities with a unified approach to protection by describing these components in the security architecture.

3 OPERATIONAL CONTROLS

3.1 (AT) Awareness and Training

3.1.1 (AT-1) Security Awareness and Training Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBIWTP operations contractors:
 - 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Reviews and updates the current:

1. Security awareness and training policy; and
2. Security awareness and training procedures bi-annually.

Implementation:

Inherited Control

The USIBWC has taken the following actions to implement a security awareness and training policy and its associated procedures:

a. A security awareness and training policy has been developed to address the following areas:

- i. Purpose
- ii. Scope,
- iii. Roles,
- iv. Responsibilities
- v. Management commitment,
- vi. Coordination among all USIBWC officials
- vii. Proper compliance.

Procedures have also been developed by USIBWC to facilitate the implementation of the security awareness and training policy and the associated security awareness and training controls. These policies and procedures have been distributed to all USIBWC employees

b. The security awareness and training policy is reviewed annually along with its associated implementation procedures.

3.1.2 (AT-2) Security Awareness

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

- a. As part of initial training for new users;
- b. When required by information system changes; and
- c. annually thereafter.

Implementation:

Inherited Control

The USIBWC takes the following actions to address security awareness:

The conditions listed below are triggers for when basic security awareness training is provided to the System users, managers, senior executives, and contractors:

- i. Basic security awareness training is provided as part of the initial training for new USIBWC information system users.
- ii. Basic security awareness training is provided to all USIBWC users when required by System changes.
- iii. Basic security awareness training is provided annually thereafter to all USIBWC employees.

AT-2(2) SECURITY AWARENESS | INSIDER THREAT

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Implementation:

Inherited Control

The USIBWC includes sections within the provided security awareness and training modules on recognizing and reporting indicators of an insider threat.

3.1.3 (AT-3) Role-Based Security Training

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

- a. Before authorizing access to the information system or performing assigned duties;
- b. When required by information system changes; and
- c. Annually thereafter.

Implementation:

System Specific Control

The USIBWC provides role-based security training to personnel with assigned security roles and responsibilities under the following conditions:

- a. Role-based security training is provided before authorizing access to the System or performing any assigned duties as part of the Security Awareness and Training modules that are distributed by USIBWC.
- b. Role-based security training is provided when required by changes to the applicable USIBWC information systems
- c. Role-based security training is provided annually thereafter. All USIBWC System users are required to complete the provided security awareness and training modules on an annual basis.

3.1.4 (AT-4) Security Training Records

Control: The organization:

- a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
- b. Retains individual training records for two years.

Implementation:

Hybrid Control

The USIBWC takes the following actions to maintain security records:

- a. Individual security training activities are monitored by the USIBWC Information Systems Security Officer including basic security awareness training and specific training that is unique to the System.

System Specific Implementation

These security training modules are designed for Industrial Control System users.

- b. Individual training records for the System users are retained for five (5) calendar years. The most recent records for this training that have been completed are included as part of this Authority to Operate (ATO) package.

3.2 (CM) Configuration Management

3.2.1 (CM-1) Configuration Management Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBIWTP operations and maintenance contractors:
 - 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
- b. Reviews and updates the current:
 - 1. Configuration management policy and;
 - 2. Configuration management procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement configuration management policy and procedures:

- a. A configuration management policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the configuration management policy and the associated configuration management controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The configuration management policy is reviewed annually along with its associated implementation procedures.

3.2.2 (CM-2) Baseline Configuration

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Implementation:

System Specific Control

The SBIWTP develops, documents, and maintains a current baseline configuration of the System. This baseline configuration consists of developer user manuals and follows the hardening guidelines of the United States Government Configuration Baseline (USGCB); it is maintained under configuration control.

CM-2(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

The organization reviews and updates the baseline configuration of the information system:

- (a) Annually;
- (b) When required due to update or upgrades; and
- (c) As an integral part of information system component installations and upgrades.

Implementation:

System Specific Control

The SBIWTP reviews and updates the baseline configuration of the System when any of the following conditions are met:

- a. It is reviewed and updated annually.
- b. It is reviewed and updated whenever a major change occurs, or in response to security control assessments/audit findings
- c. It is reviewed as an integral part of any System component installation or upgrades.

CM-2(2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Implementation:

System Specific Control

The SBIWTP employs services from the GovPlace CDM security package to detect and report changes to the System hardware. This serves as an automated mechanism to maintain an up-to-date, complete, accurate, and readily available baseline configuration for the System.

CM-2(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

The organization retains *baseline configurations of the information system* to support rollback.

Implementation:

System Specific Control

The SBIWTP retains previous versions of the System baseline configuration at ten (5) year intervals to support rollback.

CM-2(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

The organization:

- (a) Issues SCADA system components and devices with configurations to individuals traveling to locations that the organization deems to be of significant risk; and**
- (b) Applies safeguards to the devices when the individuals return.**

Implementation:

Not Applicable

The System components cannot be taken and moved to a high-risk area and returned at a later time.

3.2.3 (CM-3) Configuration Change Control

Control: The organization:

- a. Determines the types of changes to the information system that are configuration controlled;
- b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
- c. Documents configuration change decisions associated with the information system;
- d. Implements approved configuration-controlled changes to the information system;
- e. Retains records of configuration-controlled changes to the information system for 3 years;
- f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
- g. Coordinates and provides oversight for configuration change control activities through the IMD that convenes a board to review and approve changes.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address configuration change control:

- a. The types of changes to the System have been determined to be any hardware or software component that requires an upgrade or replacement.
- b. The proposed configuration-controlled changes to the System are reviewed and either approved or denied after a security impact analysis is given explicit consideration.
- c. The configuration change decisions associated with the System are documented.
- d. All approved configuration-controlled changes to the System are implemented in a timely manner.
- e. Records for configuration-controlled changes to the System are retained for a period of ten (5) years.
- f. Activities associated with the configuration-controlled changes are reviewed and audited annually.
- g. The SBIWTP coordinates and provides oversight for configuration control activities through a local Configuration Control Board (CCB) that convenes at least once per each calendar month or if a meeting is called to discuss configuration changes in greater detail.

CM-3(2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Implementation:

System Specific Control

The SBIWTP: Tests, validates, and documents all changes to the System before the changes are implemented onto the production system.

3.2.4 (CM-4) Monitoring Configuration Changes

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Implementation:

System Specific Control

The SBIWTP analyzes changes to the System by conducting security impact analyses to determine any potential security impacts prior to implementing the change.

CM-4(1) *SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Implementation:

System Specific Control

The SBIWTP analyzes change to the System in a separate test environment before implementation in the production environment. This is done for the purpose of looking for security impacts due to flaws, weaknesses, incompatibility, and intentional malice.

3.2.5 (CM-5) Access Restrictions for Change

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Implementation:

System Specific Control

The SBIWTP defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the System by:

- a. Allowing all employees to submit Requests for Change (RFC).
- b. Only allowing officials that are designated members of the CCB to vote on, approve, or deny changes to the System.
- c. Only allowing authorized officials to implement changes to the System.

CM-5(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*

The information system enforces access restrictions and supports auditing of the enforcement actions.

Implementation:

System Specific Control

The System uses a SharePoint site to enforce access restrictions for change. The SharePoint site supports the auditing of these enforcement actions.

CM-5(2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES

The organization reviews information system changes annually to determine whether unauthorized changes have occurred.

Implementation:

System Specific Control

The SBIWTP reviews change to the System on a monthly basis at every CCB meeting to determine whether unauthorized changes have occurred on the SBIWTPCADA Network.

CM-5(3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS

The information system prevents the installation *software and firmware components* without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Implementation:

System Specific Control

The SBIWTP prevents the installation of any software or firmware components without verification that the component in question has been digitally signed using a certificate that is recognized and approved by the SBIWTP.

3.2.6 (CM-6) Configuration Settings

Control: The organization:

- a. Establishes and documents configuration settings for information technology products employed within the information system using IMD provided security configuration checklists that reflect the most restrictive mode consistent with operational requirements;
- b. Implements the configuration settings;
- c. Identifies, documents, and approves any deviations from established configuration settings for information system components based on agency operational requirements; and
- d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address configuration settings in the System:

- a. The SBIWTP has established and documented configuration settings for all of the information technology products employed within the System using the USGCB and the recommended configuration settings supplied in the vendor instruction manuals. These settings reflect the most restrictive modes consistent with the operational requirements.
- b. All configuration settings that are recommended for the components of the System are implemented properly.
- c. Any deviations from the established configuration settings in the System components are identified, documented, and approved if they are consistent with the established operational requirements.
- d. All configuration settings are monitored and controlled in accordance with the System Configuration Management policy.

CM-6(2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

The organization employs change control alerts to respond to unauthorized changes to changes.

Implementation:

System Specific Control

The SBIWTP employs safeguards to respond to unauthorized changes to all System configuration settings that are defined.

3.2.7 (CM-7) Least Functionality

Control: The organization:

- a. Configures the information system to provide only essential capabilities; and
- b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services:
[Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

Implementation:

System Specific Control

The SBIWTP takes the following actions to address the concept of least functionality:

- a. The SBIWTP SCADA System is configured to provide only the essential capabilities that are commensurate with each component's function. The current open ports are listed below:
 - 18 SIP callout for SCADA Alarms
 - 65 SIP callout for SCADA Alarms
 - 71 SIP callout for SCADA Alarms
 - 74 SIP callout for SCADA Alarms
 - 81 SIP callout for SCADA Alarms
 - 194 SIP callout for SCADA Alarms
 - 254 SIP callout for SCADA Alarms
 - 512 Tofino Firewalls
 - 514 Syslog ASA
 - 518 Snare

Ports have also been blocked on the Cisco switches as necessary

- b. Legacy SCADA protocols are prohibited from use on the System.

CM-7(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

The organization:

- (a) Reviews the information system annually to identify unnecessary and/or non-secure functions, ports, protocols, and services; and**
- (b) Disables ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.**

Implementation:

System Specific Control

The SBIWTP takes the following actions to ensure that periodic review of least functionality is accomplished on the System:

- a. The System is reviewed annually to identify unnecessary and non-secure functions, ports, protocols, and services
- b. All functions, ports protocols, and services that are deemed unnecessary within the System are disabled promptly.

CM-7(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

Implementation:

System Specific Control

The System prevents program execution in accordance with the System Configuration Management Policy.

CM-7(5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING

The organization:

- (a) Identifies software programs authorized to execute on the information system;**

- (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and**
- (c) Reviews and updates the list of authorized software programs annually.**

Implementation:

System Specific Control

The SBIWTP takes the following actions to address software whitelisting on the System:

- a. The SBIWTP has identified all software programs that are authorized to run on the System.
- b. A deny-all, permit-by-exception policy has been implemented to allow the execution of authorized software programs on the System.
- c. The list of programs that are authorized to run on the System is reviewed and updated annually.

3.2.8 (CM-8) Information System Component Inventory

Control: The organization:

- a. Develops and documents an inventory of information system components that:
 - 1. Accurately reflects the current information system;
 - 2. Includes all components within the authorization boundary of the information system;
 - 3. Is at the level of granularity deemed necessary for tracking and reporting; and
 - 4. Includes information deemed necessary to achieve effective information system component accountability; and
- b. Reviews and updates the information system component inventory annually.

Implementation:

System Specific Control

The SBIWTP takes the following actions to retain a component inventory for the System:

- a. A component inventory has been developed and documented for the System. It accurately reflects the current state of the System. It includes all of the components within the current authorization boundary. It maintains an appropriate level of granularity that is necessary for tracking and reporting. The inventory does not have the appropriate level of granularity to promote proper accountability. The component inventory should include:
 - i. Models
 - ii. Serial numbers
 - iii. Cost of each component
 - iv. Location of each component.
- b. The System Component inventory is reviewed and updated annually.

CM-8(1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Implementation:

System Specific Control

The SBIWTP updates the component inventory for the System as an integral part of component installations, removals, and updates.

CM-8(2) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Implementation:

System Specific Control

The SBIWTP uses the CDM asset identification tools as automated mechanisms to assist with maintaining an up-to-date, complete, accurate, and readily available inventory of system components.

CM-8(3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

The organization:

- (a) Employs automated mechanisms annually to detect the presence of unauthorized hardware, software, and firmware components within the information system; and**
- (b) Takes the following actions when unauthorized components are detected: Disables network access.**

Implementation:

System Specific Control

The SBIWTP takes the following actions to address automated unauthorized component detection on the System:

- a. The CDM security tools provided by GovPlace Security Solutions are deployed as automated mechanisms to continuously detect the presence of unauthorized hardware, software, and firmware components within the System.
- b. Components of the System are isolated if an unauthorized component is detected. Further, a notification is sent to the System to the USIBWC ISSM.
- c. Monthly asset scans occur through the VMaaS service.

CM-8(4) INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION

The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.

Implementation:

System Specific Control

The SBIWTP provides a method of identifying all System components by the name and position of the individual responsible and accountable for administering the components. This designation by name is included in the System inventory.

CM-8(5) INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Implementation:

System Specific Control

The SBIWTP verifies that all components within the System authorization boundary are not duplicated within the established component inventory.

3.2.9 (CM-9) Configuration Management Plan

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

- a. Addresses roles, responsibilities, and configuration management processes and procedures;
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- c. Defines the configuration items for the information system and places the configuration items under configuration management; and
- d. Protects the configuration management plan from unauthorized disclosure and modification.

Implementation:

System Specific Control

- a. The SBIWTP has developed, documented, and implemented, a Configuration Management Plan (CMP) for the System that addresses the following:
- b. The roles, responsibilities, and configuration management processes are addressed in the CMP.
- c. A process is established for identifying configuration items throughout the SDLC for managing the configuration of the configuration items. The configuration items are defined for the System and these items are placed under configuration management.
- d. The CMP is protected from unauthorized disclosure or modification. This is accomplished by only allowing those with the proper access privileges to access the CMP.

3.2.10 (CM-10) Software Usage Restrictions

Control: The organization:

- a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
- b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Implementation:

System Specific Control

The SBIWTP takes the following actions to establish software usage restrictions on the System:

- a. All software and its associated documentation are used in accordance with contract agreements and copyright laws.
- b. The use of software and its associated documentation is tracked and protected by quantity licenses to control copying and distribution.
- c. The use of peer-to-peer file-sharing technology is controlled and documented to ensure that the capability is not used for unauthorized distribution, display, performance, or reproduction of any copyrighted work.

3.2.11 . (CM-11) User Installed Software

Control: The organization:

- a. Establishes controls governing the installation of software by users;
- b. Enforces software installation policies through pre-approval; and
- c. Monitors policy compliance annually.

Implementation:

System Specific Control

The SBIWTP takes the following actions to govern the use of user installed software by users.

- a. The System Configuration Management Policy governs the installation of software by users.
- b. Software installation policies are enforced by not allowing users to install software on any System device.
- c. Policy compliance is monitored annually.

3.3 (CP) Contingency Planning

3.3.1 (CP-1) Contingency Planning Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 - 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
- b. Reviews and updates the current:
 - 1. Contingency planning policy and
 - 2. Contingency planning procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement contingency planning policy and procedures:

- a. A contingency planning policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the contingency planning policy and the associated contingency planning controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The contingency planning policy is reviewed annually along with its associated implementation procedures.

3.3.2 (CP-2) Contingency Plan

Control: The organization:

- a. Develops a contingency plan for the information system that:
 - 1. Identifies essential missions and business functions and associated contingency requirements;
 - 2. Provides recovery objectives, restoration priorities, and metrics;
 - 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
 - 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
 - 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
 - 6. Is reviewed and approved by SBITWP operations and SCADA maintenance contractors;
- b. Distributes copies of the contingency plan to SBIWTP operations and SCADA system maintenance contractors;
- c. Coordinates contingency planning activities with incident handling activities;
- d. Reviews the contingency plan for the information system annually;
- e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- f. Communicates contingency plan changes to SBIWTP operations and SCADA system maintenance contractors; and
- g. Protects the contingency plan from unauthorized disclosure and modification.

Implementation:

System Specific Control

The SBIWTP has developed a contingency plan for the System that addresses the following:

- a. All essential mission and business functions along with their associated business requirements have been identified. Recovery objectives, restoration priorities, and metrics have been provided. Contingency roles, responsibilities have been assigned to

specific individuals. Their contact information has been provided. The continuity of essential missions and business functions during a disruption, compromise, or failure have also been addressed. Full information system restoration processes have been incorporated that include minimal deterioration of the original security safeguards that were planned and implemented. Finally, the contingency plan is reviewed and approved by both the System Owner and the ISSM.

- b. Copies of the contingency plan have been distributed to the System Owner and the ISSM.
- c. Contingency planning activities are coordinated with incident handling activities on the System.
- d. The System contingency plan is reviewed annually at a minimum, whenever there is a major change to the system or whenever an incident occurs that warrants an update to incorporate lessons learned.
- e. The contingency plan is updated to address changes to the SBIWTP and/or the IBWC, the environment of operation, and any problems that are encountered during the contingency plan implementation, execution, or testing.
- f. Contingency plan changes are communicated to the System owner, ISSM, and any other relevant stakeholders that are identified and who participate in the continuity of operations.
- g. The contingency plan is protected from unauthorized disclosure and modification by placing it in a SharePoint security archive that is only accessible to authorized officials.

CP-2(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Implementation:

System Specific Control

The SBIWTP coordinates the development of the System contingency plan with the system's incident response plan.

CP-2(2) CONTINGENCY PLAN | CAPACITY PLANNING

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Implementation:

System Specific Control

The SBIWTP has conducted capacity planning on the System so that the necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2(3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of essential missions and business functions within two hours of contingency plan activation.

Implementation:

System Specific Control

The SBIWTP plans for the resumption of essential missions and business functions of the System within two (2) hours of contingency plan activation.

CP-2(4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of all missions and business functions within two hours of contingency plan activation.

Implementation:

System Specific Control

The SBIWTP plans for the resumption of all missions and business functions of the System within eight (8) hours of contingency plan activation.

CP-2(5) CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Implementation:

System Specific Control

The SBIWTP plans for the continuity of essential missions and business functions of the System with little or no loss of operational continuity. The continuity is sustained until full system restoration at the primary processing and storage sites is possible.

CP-2(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

The organization identifies critical information system assets supporting essential missions and business functions.

Implementation:

System Specific Control

The SBIWTP identifies critical System assets that support the essential missions and business functions of the wastewater treatment facility.

3.3.3 (CP-3) Contingency Training

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

- a. Within 30 days of assuming a contingency role or responsibility;
- b. When required by information system changes; and
- c. annually thereafter.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address contingency training:

- a. Contingency training is provided within one (1) week of an employee assuming a contingency role or responsibility.
- b. Contingency training is provided when changes are made to the System
- c. Contingency training is provided annually thereafter.

CP-3(1) CONTINGENCY TRAINING | SIMULATED EVENTS

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Implementation:

System Specific Control

The SBIWTP incorporates simulated events into the System contingency training to facilitate an effective response by SBIWTP/IBWC personnel in crisis situations.

3.3.4 (CP-4) Contingency Plan Testing

Control: The organization:

- a. Tests the contingency plan for the information system annually using annual tests to determine the effectiveness of the plan and the organizational readiness to execute the plan;
- b. Reviews the contingency plan test results; and
- c. Initiates corrective actions, if needed.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address contingency plan testing for the System:

- a. The contingency plan is tested annually using a rotation of contingency plan tests on a year by year basis. These are used to determine the effectiveness of the plan as well as SBIWTP's/IBWC's readiness to execute the contingency plan.
 - i. A table-top exercise
 - ii. Functional Exercise
- b. After the test is completed the results are reviewed to discuss any lessons learned.
- c. Corrective actions are initiated and implemented if necessary.

CP-4(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Implementation:

System Specific Control

The SBIWTP coordinates contingency plan testing with incident response elements responsible for the incident response plan.

CP-4(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

The organization tests the contingency plan at the alternate processing site:

- (a) To familiarize contingency personnel with the facility and available resources; and**
- (b) To evaluate the capabilities of the alternate processing site to support contingency operations.**

Implementation:

System Specific Control

The SBIWTP tests the contingency plan at the alternate processing site. The purpose is to familiarize all relevant personnel with the facility and available resources. The other purpose is to evaluate the capabilities of the alternate processing site to support contingency operations.

CP-4(4) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Implementation:

System Specific Control

The SBIWTP includes a full recovery and reconstruction capability of the System to a known state as part of contingency plan testing.

3.3.5 (CP-6) Alternate Storage Site

Control: The organization:

- a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

- b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Implementation:

System Specific Control

The SBIWTP takes the following actions to set up an alternate storage site:

- a. An alternate storage site has been established that includes the necessary agreements to permit the storage and retrieval of the System backup information.
- b. The alternate storage site for the System provides information security controls that are at the equivalent level of the primary site.

CP-6(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Implementation:

System Specific Control

The SBIWTP has identified an alternate storage site that is separated from the primary storage site to reduce the susceptibility to the same threats. The SBIWTP leverages the GovPlace datacenter as the alternate storage site for the SBIWTP SCADA System.

CP-6(2) ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Implementation:

System Specific Control

The SBIWTP has configured the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

CP-6(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Status: This control is currently associated with POA&M #1

Implementation:

System Specific Control

The SBIWTP leverages the GovPlace datacenter as the alternate storage site for the SBIWTP SCADA System. Documentation will be obtained that evaluates specific risks to the site itself an area-wide disruption occurs.

This control is part of a POA&M.

CP-8(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

The organization:

- (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
- (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address the priority of service provisions:

- a. Both primary and alternate telecommunications service agreements that contain priority of service provisions in accordance with the SBIWTP availability requirements; these include the recovery time objectives.
- b. Telecommunications service priority has been requested for all telecommunications services used for the purpose of national security emergency preparedness because the primary and alternate telecommunications services are provided by a common carrier.

CP-8(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Implementation:

System Specific Control

The SBIWTP has obtained an alternate telecommunications service to reduce the likelihood of sharing a single point of failure with the primary telecommunications service.

CP-8(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Implementation:

System Specific Control

The SBIWTP has obtained an alternate telecommunications services from providers that are separated from the primary service providers to reduce the susceptibility of the same threats.

CP-8(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Implementation:

System Specific Control

The SBIWTP has obtained alternate telecommunication services from providers that are separated from primary service providers to reduce the susceptibility to the same threats.

CP-8(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

The organization:

- (a) Requires primary and alternate telecommunications service providers to have contingency plans;**
- (b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and**
- (c) Obtains evidence of contingency testing/training by providers annually.**

Implementation:

System Specific Control

The SBIWTP has taken the following actions to obtain a telecommunications service provider contingency plan:

- a. The SBIWTP has required that the primary and alternate and telecommunications service providers to provide their own contingency plans.
- b. The SBIWTP reviews the telecommunications provider contingency plan to ensure that the contingency plan meets SBIWTP's contingency requirements.
- c. SBIWTP has obtained evidence that contingency plan training has been given by the provider annually.

3.3.6 (CP-9) Information System Backup

Control: The organization:

- a. Conducts backups of user-level information contained in the information system daily;
- b. Conducts backups of system-level information contained in the information system on a monthly basis;
- c. Conducts backups of information system documentation including security-related documentation quarterly; and
- d. Protects the confidentiality, integrity, and availability of backup information at off-site storage locations.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address information system backup for the System:

- a. The SBIWTP conducts backups of user level information weekly, which is consistent with the recovery time and recovery point objectives. The user-level information includes user accounts and passwords.
- b. Backups of SCADA supervisory information is conducted daily. The SCADA supervisory data is currently the only information that has been identified as relevant system-level data.
- c. Information system documentation is backed up daily at a minimum. This is consistent with recovery time and recovery point objectives.
- d. The confidentiality, integrity, and availability of backup information are protected at the backup storage locations.

CP-9(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY

The organization tests backup information annually to verify media reliability and information integrity.

Status: This control is currently associated with POA&M #2

Implementation:

System Specific Control

The SBIWTP tests backup information for the SBIWTP SCADA System annually to verify media reliability and information integrity.

CP-9(2) INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Implementation:

System Specific Control

The SBIWTP uses a sample of backup information in the restoration of selected information system functions as part of the contingency plan testing. A sampling of information was conducted in the fall of 2016 as part of the annual Contingency Plan Testing. The test was successful supporting backup system integrity and validation of information.

CP-9(3) INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

The organization stores backup copies of *critical information system software and other security-related information* in an off-site facility or in a fire-rated container that does not collocate with the operational system.

Implementation:

System Specific Control

The SBIWTP stores backup copies of SCADA information from the System in a separate facility in a fire-rated container that does not collocate with the operational SCADA Network.

CP-9(5) *INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*

The organization transfers information system backup information to an alternate storage site monthly.

Implementation:

System Specific Control

The SBIWTP transfers the System backup information to the alternate storage site at a transfer rate that is consistent with the recovery time and the recovery point objectives.

3.3.7 (CP-10) Information System Recovery and Reconstitution

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Implementation:

System Specific Control

The SBIWTP provides for the recovery and reconstruction of the System after a disruption, compromise, or failure. Documentation for a full recovery and reconstruction procedures is currently being developed.

CP-10(2) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*

The information system implements transaction recovery for systems that are transaction-based.

Implementation:

System Specific Control

The SBIWTP SCADA System provides transaction recovery for all transactions from the field devices to the HMIs.

CP-10(4) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*

The organization provides the capability to restore information system components within four hours from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Implementation:

System Specific Control

The SBIWTP provides the capability to restore the System components within the appropriately defined restoration time periods as defined in the contingency plan. All restoration procedures are taken from information that is configuration controlled and integrity protected and it represents a known operational state of the System components.

3.4 (IR) Incident Response

3.4.1 (IR-1) Incident Response Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
- b. Reviews and updates the current:
 1. Incident response policy annually; and
 2. Incident response procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement incident response policy and procedures:

- a. An incident response policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the incident response policy and the associated incident response controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The incident response policy is reviewed annually along with its associated implementation procedures.

3.4.2 (IR-2) Incident Response Training

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

- a. Within 30 days of assuming an incident response role or responsibility;
- b. When required by information system changes; and
- c. annually thereafter.

Implementation:

System Specific Control

The SBIWTP provides incident response training to the System users that are consistent with the defined roles and responsibilities. This training is issued under the following conditions:

- a. Training is provided within one (1) week of assuming an incident role or responsibility.
- b. Refresher incident response training is provided as required whenever a significant change occurs to the System.
- c. Subsequent training is provided annually thereafter.

IR-2(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Implementation:

System Specific Control

The SBIWTP incorporates simulated events into the System incident response training to facilitate an effective response by personnel in crisis situations.

IR-2(2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms in the System to provide a more thorough and realistic incident response training environment.

3.4.3 (IR-3) Incident Response Testing and Exercises

Control: The organization tests the incident response capability for the information system annually using simulation tests to determine the incident response effectiveness and documents the results.

Implementation:

System Specific Control

The SBIWTP tests the incident response capability of the System annually using the defined incident response tests to determine the effectiveness of the incident response function. The results are documented appropriately.

IR-3(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

The organization coordinates incident response testing with organizational elements responsible for related plans.

Implementation:

System Specific Control

The SBIWTP coordinates the System with the contingency planning elements and the contingency test plans.

3.4.4 (IR-4) Incident Handling

Control: The organization:

- a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- b. Coordinates incident handling activities with contingency planning activities; and
- c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to incorporate an incident handling process for the System:

- a. An incident handling capability is implemented for security incidents that include preparation, detection/analysis, containment, eradication, and recovery.
- b. Incident handling activities are coordinated with contingency planning activities
- c. Lessons learned are incorporated into the incident response testing, training, and supporting procedures that are taken from ongoing incident handling activities. All changes resulting from these lessons learned are implemented accordingly.

IR-4(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

The organization employs automated mechanisms to support the incident handling process.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms on the System that are deployed through the CDM tools to support the incident handling process.

IR-4(4) INCIDENT HANDLING | INFORMATION CORRELATION

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Implementation:

System Specific Control

The SBIWTP correlates incident information from the System's individual incident responses to achieve an IBWC wide perspective on incident awareness and response.

3.4.5 (IR-5) Incident Monitoring

Control: The organization tracks and documents information system security incidents.

Implementation:

System Specific Control

The SBIWTP tracks and documents all security incidents for the System.

IR-5(1) INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms for the System using services provided by the CDM tools. These mechanisms assist with tracking security incidents and they also support the collection and analysis of incident information.

3.4.6 (IR-6) Incident Reporting

Control: The organization:

- a. Requires personnel to report suspected security incidents to the organizational incident response capability within one hour]; and
- b. Reports security incident information to the IMD.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address incident reporting:

- a. All personnel is required to report suspected security incidents to the SBIWTP incident response capability within four (4) hours of the initial discovery.
- b. Security incident information is reported to the System Owner, ISSM, and the GovPlace CDM staff.

IR-6(1) INCIDENT REPORTING | AUTOMATED REPORTING

The organization employs automated mechanisms to assist in the reporting of security incidents.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms on the System to assist with reporting security incidents. These automated mechanisms are taken from the GovPlace CDM services.

3.4.7 (IR-7) Incident Response Assistance

Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Implementation:

System Specific Control

The SBIWTP provides the GovPlace CDM services as an incident response resource as an integral part of the SBIWTP incident response capability. It offers advice and assistance to users of the System for the handling and reporting of security incidents.

IR-7(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms to increase the availability of incident response-related information and support for the System. These mechanisms are taken from the GovPlace CDM services.

3.4.8 (IR-8) Incident Response Plan

Control: The organization:

- a. Develops an incident response plan that:
 1. Provides the organization with a roadmap for implementing its incident response capability;
 2. Describes the structure and organization of the incident response capability;
 3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
 5. Defines reportable incidents;
 6. Provides metrics for measuring the incident response capability within the organization;
 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
 8. Is reviewed and approved by SBITWP operations and SCADA maintenance contractors ;
- b. Distributes copies of the incident response plan to SBIWTP operations and SCADA system maintenance contractors;
 - c. Reviews the incident response plan annually;
 - d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
 - e. Communicates incident response plan changes to SBIWTP operations and maintenance contractors; and
 - f. Protects the incident response plan from unauthorized disclosure and modification.

Implementation:

System Specific Control

The SBIWTP has developed an incident response plan for the System that addresses the following:

- a. It provides the SBIWTP with a roadmap for implementing its incident response capability for the System. The structure and organization of the incident response capability are also described. A high-level approach is also provided to describe how the incident response capability fits into the entirety of SBIWTP. It meets the unique requirements of the SBIWTP which relate to the mission, size, structure, and functions. It defines incidents that are reportable. It also provides metrics for measuring the incident response capability within the SBIWTP. The incident response plan is reviewed and approved by the SBIWTP system owner and the ISSM.
- b. Copies of the incident response plan are distributed to the System Owner, ISSM, and the AO
- c. The incident response plan is reviewed annually.
- d. The incident response plan is updated to address the System and SBIWTP/IBWC organizational changes and any problems that were encountered during the implementation, execution, and testing of the plan.
- e. Changes to the incident response plan are communicated to the System Owner, the ISSM, the AO, and the GovPlace CDM staff.
- f. The incident response plan is protected from unauthorized disclosure and modification by only allowing authorized personnel to access the plan.

3.5 (MA) Maintenance

3.5.1 (MA-1) System Maintenance Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBIWTP Operations and maintenance contractors:
 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
- b. Reviews and updates the current:
 1. System maintenance policy annually; and
 2. System maintenance procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement system maintenance policy and procedures:

- a. A system maintenance policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the system maintenance policy and the associated system maintenance controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The system maintenance policy is reviewed annually along with its associated implementation procedures.

3.5.2 (MA-2) Controlled Maintenance

Control: The organization:

- a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- c. Requires that IMD explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
- d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
- f. Includes maintenance-related information in organizational maintenance records.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address controlled maintenance on the System:

- a. Records of maintenance and repairs are scheduled, performed, reviewed, and documented on the System components in accordance with manufacturer and vendor specifications along with SBIWTP requirements.
- b. Approves and monitors all maintenance activities whether they are performed onsite or remotely and whether the equipment that is serviced is corrected on site or removed to another location.
- c. The SBIWTP system owner is explicitly required to approve the removal of the System components from SBIWTP facilities for off-site maintenance and/or repairs.
- d. All potentially impacted security controls are checked to verify that the controls are still functioning properly upon completion the maintenance and repair activities.
- e. All information related to the specific maintenance activity is required to be present in the System maintenance records.

MA-2(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

The organization:

- (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and**
- (b) Produces up-to-date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in the process, and completed.**

Implementation:

System Specific Control

The SBIWTP has taken the following actions to allow automated maintenance activities.

- a. Automated schedules are used as the automated mechanisms to schedule, conduct, and document maintenance and repairs.

- b. The SBIWTP and its associated maintenance contractors produce up-to-date, accurate, and complete records of maintenance and repair actions that are either requested, scheduled, in the process, and completed.

3.5.3 (MA-3) Maintenance Tools

Control: The organization approves, controls, and monitors information system maintenance tools.

Status: This control is currently associated with POA&M #3

Implementation:

System Specific Control

The SBIWTP approves, controls, and monitors all maintenance tools for the System.

MA-3(1) MAINTENANCE TOOLS | INSPECT TOOLS

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Implementation:

System Specific Control

The SBIWTP inspects all maintenance tools carried into an SBIWTP facility by maintenance personnel. These tools are inspected for unauthorized and/or improper modifications.

MA-3(2) MAINTENANCE TOOLS | INSPECT MEDIA

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Implementation:

System Specific Control

The SBIWTP checks all media that contains diagnostic and test programs for malicious code before the media are used in the System.

MA-3(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

- (a) Verifying that there is no organizational information contained on the equipment;
- (b) Sanitizing or destroying the equipment;
- (c) Retaining the equipment within the facility; or
- (d) Obtaining an exemption from IMD explicitly authorizing the removal of the equipment from the facility.

Implementation:

System Specific Control

The SBIWTP takes the following actions to prevent unauthorized removal of maintenance equipment that contains SBIWTP information.

- a. All maintenance equipment is scanned and verified that there is no SBIWTP/IBWC information contained on the maintenance equipment prior to removal.
- b. All maintenance equipment is either sanitized or destroyed prior to removal
- c. Any maintenance equipment that contains SBIWTP may be retained within the facility as necessary.
- d. No exceptions are allowed to remove maintenance equipment from an SBIWTP facility that contains SBIWTP related information.

3.5.4 (MA-4) Remote Maintenance

Control: The organization:

- a. Approves and monitors nonlocal maintenance and diagnostic activities;
- b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

- c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- d. Maintains records for nonlocal maintenance and diagnostic activities, and
- e. Terminates session and network connections when nonlocal maintenance is completed.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address remote maintenance concerns:

- a. All nonlocal maintenance and diagnostic activities are approved and monitored.
- b. Nonlocal maintenance and diagnostic tools are only allowed insofar as they are consistent with SBIWTP policies and documented within this security plan.
- c. Strong authenticators are employed during the establishment of nonlocal maintenance and diagnostic sessions.
- d. Records for nonlocal maintenance and diagnostic activities are maintained.
- e. Session and network connections are terminated when the nonlocal maintenance activity or activities are completed.

MA-4(2) NONLOCAL MAINTENANCE / DOCUMENT NONLOCAL MAINTENANCE

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Implementation:

System Specific Control

MA-4(3) NONLOCAL MAINTENANCE / COMPARABLE SECURITY / SANITIZATION

The organization:

- (a) Requires that nonlocal maintenance and diagnostic services be performed by an information system that implements a security capability comparable to the capability implemented on the system being serviced; or**
- (b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.**

Implementation:

System Specific Control

The SBIWTP takes the following actions to ensure that nonlocal maintenance activities have comparable security and sanitization procedures.

- a. All nonlocal maintenance and diagnostic services are required to be performed by an information system that implements a security capability comparable to the capability of security that is implemented on the System.
- b. The component to be serviced is removed from the System prior to the nonlocal maintenance or diagnostic activities. The component is sanitized of any SBIWTP information if it must be removed from an SBIWTP facility. After the activity is complete, the component is inspected and sanitized to prevent malicious software from entering the SBIWTP facility before reconnecting the component to the System.

3.5.5 (MA-5) Maintenance Personnel

Control: The organization:

- a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

- c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address concerns with maintenance personnel:

- a. A process is established for authorizing maintenance personnel. Further, a list of authorized maintenance personnel and organizations are maintained.
- b. Non-escorted personnel that performs maintenance activities on the System have the appropriate access authorizations.
- c. Proper SBIWTP personnel with the appropriate access authorizations and technical competence are designated to supervise the maintenance personnel who do not possess the required access authorizations for the System.

MA-5(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

The organization:

- (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens that include the following requirements:**
 - (1) Maintenance personnel who do not have needed access authorizations, clearances or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;**
 - (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and**
- (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.**

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement procedures for maintenance individuals without appropriate access.

- a. Procedures have been implemented for the use of maintenance personnel that lack the appropriate security clearances or who are not U.S. citizens. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted by SBIWTP personnel. Further, this personnel is supervised during the performance of all maintenance and diagnostic activities on the System by approved SBIWTP personnel. This personnel are fully cleared, have appropriate access authorizations, and are technically qualified. All volatile storage components within the System are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured prior to any maintenance and diagnostic activities occurring.
- b. Alternate security safeguards are implemented in the event a system component cannot be sanitized, removed, or disconnected from the system.

3.5.6 (MA-6) Timely Maintenance

Control: The organization obtains maintenance support and/or spare parts for SCADA system components within 24 hours of failure.

Implementation:

System Specific Control

The System obtains maintenance support and spare parts for all System equipment. This equipment is obtained within one (1) week of failure.

3.6 (MP) Media Protection

3.6.1 (MP-1) Media Protection Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
- b. Reviews and updates the current:
 1. Media protection policy annually; and
 2. Media protection procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement a media protection policy and procedures:

- a. A media protection policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the media protection policy and the associated media protection controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The media protection policy is reviewed annually along with its associated implementation procedures.

3.6.2 (MP-2) Media Access

Control: The organization restricts access to digital configuration media of the SBITWP operations and SCADA maintenance contractors .

Implementation:

System Specific Control

The SBIWTP restricts access to all System equipment to only the SBIWTP employees and/or support personnel who require access to the System.

3.6.3 (MP-3) Media Labeling

Control: The organization:

- a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- b. Exempts ControlLogix configurations as long as the media remain within the SBIWTP controlled areas].

Implementation:

System Specific Control

The SBIWTP takes the following actions to ensure proper media labeling for the System equipment.

- a. All System media is marked indicating the distribution limitations, handling caveats, and applicable security markings of the System information.
- b. No System equipment is exempted from labeling under any circumstances.

3.6.4 (MP-4) Media Storage

Control: The organization:

- a. Physically controls and securely stores configuration media within the SBIWTP; and
- b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Status:

Implementation:

System Specific Control

The SBIWTP takes the following actions to control media storage for the System equipment:

- a. All System media is physically controlled and securely stored within either the System control room or the administration building and
- b. All System media is protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3.6.5 (MP-5) Media Transport

Control: The organization:

- a. Protects and controls information media during transport;
- b. Maintains accountability for information system media during transport outside of controlled areas;
- c. Documents activities associated with the transport of information system media; and
- d. Restricts the activities associated with the transport of information system media to authorized personnel.

Implementation:

System Specific Control

The SBIWTP takes the following actions to account for System media transport.

- a. All System media is protected and controlled during transport outside of controlled areas using the appropriate safeguards
- b. An accounting for all System media is maintained during transport outside of any controlled area.
- c. All activities associated with the transport of System media are documented.
- d. All activities associated with the transport of the System media are restricted to authorized personnel.

MP-5(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Implementation:

System Specific Control

The System implements the appropriate cryptographic mechanisms to protect the confidentiality and integrity of the System information stored on digital media during transport outside of controlled areas.

3.6.6 (MP-6) Media Sanitization and Disposal

Control: The organization:

- a. Sanitizes server and client hard drives prior to disposal, release out of organizational control, or release for reuse using standard sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and

- b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Implementation:

System Specific Control

The SBIWTP takes the following actions to ensure that proper media sanitization and disposal procedures are in place for the System:

1. All System equipment is sanitized prior to disposal or before it is released from SBIWTP control. The proper media sanitization procedures are used in accordance with applicable standards and policies.
2. Sanitization mechanisms are employed with the strength and integrity commensurate with the security FIPS 199 criticality watermark of High.

MP-6(1) *MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Implementation:

System Specific Control

The SBIWTP reviews, approves, tracks, documents, and verifies all media sanitization and disposal actions on the System.

MP-6(2) *MEDIA SANITIZATION | EQUIPMENT TESTING*

The organization tests sanitization equipment and procedures annually to verify that the intended sanitization is being achieved.

Implementation:

System Specific Control

The SBIWTP tests all sanitization equipment and procedures annually to verify that the intended sanitization is being achieved on the System.

MP-6(3) *MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system when they reach their end of life.

Implementation:

System Specific Control

The SBIWTP applies nondestructive sanitization techniques to all portable storage devices prior to connecting them to the System under the following circumstances:

1. Whenever a portable device leaves an SBIWTP facility
2. Prior to the portable device returning to the facility

3.6.7 (MP-7) Media Use

Control: The organization restricts the use USB external hard drives unless authorized by the IMD..

Implementation:

System Specific Control

The SBIWTP prohibits the use of personal electronic media (Bring Your Own Device [BYOD]) on the System components by disabling external Universal Serial Bus (USB) ports.

MP-7(1) *MEDIA USE | PROHIBIT USE WITHOUT OWNER*

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Implementation:

System Specific Control

The SBIWTP prohibits the use of all portable storage devices in the System when these devices have no identifiable owner.

3.7 (PE) Physical and Environmental Protection

3.7.1 (PE-1) Physical and Environmental Protection Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
- b. Reviews and updates the current:
 1. Physical and environmental protection policy annually; and
 2. Physical and environmental protection procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement a media protection policy and procedures:

- a. A physical and environmental policy have been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the physical and environmental policy and the associated physical and environmental controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The physical and environmental policy are reviewed annually along with its associated implementation procedures.

3.7.2 (PE-2) Physical Access Authorizations

Control: The organization:

- a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
- b. Issues authorization credentials for facility access;
- c. Reviews the access list detailing authorized facility access by individuals annually; and
- d. Removes individuals from the facility access list when access is no longer required.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to address physical access authorizations on the System:

- a. Develops, approves, and maintains A list of individuals with authorized access to the facility where the information system resides have been developed, approved and maintained for all SBIWTP employees and supporting contractors;
- b. Authorization credentials have been for facility access only to the individuals requiring access.
- c. The access list detailing authorized facility access by individuals is reviewed annually
- d. Individuals are removed from the facility access list when access is no longer required.

3.7.3 (PE-3) Physical Access Control

Control: The organization:

- a. Enforces physical access authorizations at SCADA system entry points by;
 1. Verifying individual access authorizations before granting access to the facility; and
 2. Controlling ingress/egress to the facility using agency assigned PIV cards;
- b. Maintains electronic access audit logs for entry/exit points;
- c. Provides controls to control access to SCADA system areas;
- d. Escorts visitors and monitors visitor activity to SCADA system areas and requires visitor escorts and monitoring;
- e. Secures keys, combinations, and other physical access devices;

- f. Inventories keys and other PIV alternate physical access devices annually; and
- g. Changes combinations and keys annually when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address physical access control for the System:

- a. Physical access authorizations are enforced at all entry/exit points to the facilities where the System resides. Individual access authorizations are verified before access is granted to the facility. Both ingress and egress to the facility are controlled using CAC cards and security guards.
- b. Physical access audit logs are maintained for all entry and exit points of the SBIWTP facilities where the System resides.
- c. Any facilities that have areas that are designated as publicly accessible have provided the appropriate security safeguards.
- d. Visitors are escorted and all visitor activity is monitored whenever a visitor requires access to the System.
- e. All physical access devices are secured including keys, combinations, and CAC access cards.
- f. The inventory of all physical access devices is updated annually. Combinations and keys are changed every six (6) months and/or when keys are lost, combinations are compromised, or individuals that use these combinations and keys are transferred or terminated.

PE-3(1) *PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at SCADA control areas containing one or more components of the System.

Implementation:

System Specific Control

The SBIWTP enforces all physical access authorizations to the System in addition to the physical access controls for the facilities wherever there is a facility containing one or more components of the System.

3.7.4 (PE-4) Access Control for Transmission Medium

Control: The organization controls physical access to wiring or communications media or system distribution and transmission lines within the SBIWTP facilities using metal conduit or control chasis where feasible.

Implementation:

System Specific Control

The SBIWTP controls physical access to the System distribution and transmission lines within SBIWTP facilities using the appropriate security safeguards.

3.7.5 (PE-5) Access Control for Output Devices

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Implementation:

System Specific Control

The SBIWTP controls physical access to the System output devices such as the Human Machine interfaces (HMI) to prevent unauthorized individuals from obtaining the output.

3.7.6 (PE-6) Monitoring Physical Access

Control: The organization:

- a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
- b. Reviews physical access logs annually and upon occurrence of unauthorized access; and
- c. Coordinates results of reviews and investigations with the organizational incident response capability.

Implementation:

System Specific Control

- a. The SBIWTP takes the following actions to monitor physical access to the System facilities:
- b. Physical access to the facilities is monitored where the System resides to detect and respond to physical security incidents;
- c. Physical access logs are reviewed weekly and upon occurrence of any physical security event or whenever there are potential indications of physical security events]; and
- d. The results of the reviews of the physical access logs and investigations are coordinated with the SBIWTP incident response capability.

PE-6(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

The organization monitors physical intrusion alarms and surveillance equipment.

Implementation:

System Specific Control

The SBIWTP monitors physical intrusion alarms and surveillance equipment on the System.

PE-6(4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility *containing one or more components of the SCADA system*.

Implementation:

System Specific Control

The SBIWTP monitors physical access to the System in addition to the physical access monitoring of the facility for any physical spaces containing one or more components of the information system.

3.7.7 (PE-8) Access Records

Control: The organization:

- a. Maintains visitor access records to the facility where the information system resides; and
- b. Reviews visitor access records annually.

Implementation:

System Specific Control

The SBIWTP takes the following actions to account for access records to the SBIWTP facilities where the System resides:

- a. Visitor access records are maintained at the facility where the System resides for one (1) year.
- b. All visitor access records are reviewed weekly.

PE-8(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Implementation:

System Specific Control

The SBIWTP employs automated sign-in and sign-out mechanisms to facilitate the maintenance and review of visitor access records at the facilities where the System resides.

3.7.8 (PE-9) Power Equipment and Power Cabling

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Implementation:

System Specific Control

The SBIWTP protects power equipment and power cabling for the System from damage and destruction by using protective shielding around the cabling.

3.7.9 (PE-10) Emergency Shutoff

Control: The organization:

- a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
- b. Places emergency shutoff switches or devices within SCADA System control rooms to facilitate safe and easy access for personnel; and
- c. Protects emergency power shutoff capability from unauthorized activation.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address emergency shutoff for the System:

- a. The capability of shutting off power is provided to the System or individual system components in emergency situations;
- b. The emergency shutoff switches and devices are placed in locked safes with combinations to facilitate safe and easy access to the appropriate personnel
- c. The emergency power shutoff capability is from unauthorized activation by only disclosing the safety access lock combinations to authorized personnel.

3.7.10 (PE-11) Emergency Power

Control: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

Implementation:

System Specific Control

The SBIWTP provides a short-term uninterruptible power supply to the System facilities for the purpose of facilitating an orderly shutdown of the System if necessary, and to the transition to the information system to long-term alternate power. This assists with recovering from a primary power source loss.

PE-11(1) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Implementation:

System Specific Control

The SBIWTP provides a long-term alternate power supply for the System that is capable of maintaining the minimally required operational capability in the event of an extended loss of the primary power source.

3.7.11 (PE-12) Emergency Lighting

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Implementation:

System Specific Control

The SBIWTP employs and maintains an automatic emergency lighting solution for the System that activates in the event of a power outage or disruption. The emergency lighting covers emergency exits and evacuation routes within every facility where the System resides.

3.7.12 (PE-13) Fire Protection

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Implementation:

System Specific Control

The System employs and maintains fire suppression and detection systems for the System. These systems are supported by an independent energy source.

PE-13(1) *FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*

The organization employs fire detection devices/systems for the information system that activate automatically and notifies SBIWTP operations and SCADA maintenance contractors in the event of a fire.

Implementation:

System Specific Control

The SBIWTP employs fire detection systems for the System that activates automatically and notifies the facility managers and all of the assigned emergency responders in the event of a fire.

PE-13(2) *FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to SBIWTP operations and SCADA system maintenance contractors and local emergency responders.

Implementation:

System Specific Control

The SBIWTP employs fire suppression/systems for the System that provides an automatic notification of any activation to the facility managers and all of the assigned emergency responders.

PE-13(3) *FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Implementation:

System Specific Control

The SBIWTP employs an automatic fire suppression system for the System when the facility is not staffed on a continuous interval.

3.7.13 (PE-14) Temperature and Humidity Controls

Control: The organization:

- a. Maintains temperature and humidity levels within the facility where the information system resides; and
- b. Monitors current temperature and humidity levels.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address temperature and humidity controls:

- a. The temperature and humidity levels are maintained within the facility where the System resides at the acceptable levels
- b. The temperature and humidity levels are monitored continuously by a thermostat system.

3.7.14 (PE-15) Water Damage Protection

Control: The organization protects the information system from damage resulting from water leakage by providing master shut-off or isolation valves that are accessible, working properly, and known to key personnel.

Implementation:

System Specific Control

The SBIWTP protects the System from damage resulting from water leakage by providing master shutoff and isolation valves. These valves are accessible, working properly, and known to the facility manager, all assigned maintenance personnel and all assigned emergency responders.

PE-15(1) *WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts SBITWP operations and SCADA maintenance contractors .

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms to detect the presence of water in the vicinity of System and alerts the facility manager and the assigned emergency responders.

3.7.15 (PE-16) Delivery & Removal

Control: The organization authorizes, monitors, and controls SCADA system components entering and exiting the facility and maintains records of those items.

Implementation:

System Specific Control

The SBIWTP authorizes, monitors, and all types of System components that entering and exit the SBIWTP facilities; records of those items are also maintained.

3.7.16 (PE-18) Location of Information System Components

Control: The organization positions information system components within the facility to minimize potential damage from access to minimize the opportunity for unauthorized access.

Implementation:

System Specific Control

The SBIWTP positions the System components within the facility to minimize potential damage from water and fire hazards. System components are also positioned to minimize the opportunity for unauthorized access.

3.8 (PS) Personnel Security

3.8.1 (PS-1) Personnel Security Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
- b. Reviews and updates the current:
 1. Personnel security policy annually; and
 2. Personnel security procedures annually.

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement a media protection policy and procedures:

- a. A personnel security policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the personnel security policy and the associated personnel security controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The personnel security policy is reviewed annually along with its associated implementation procedures.

3.8.2 (PS-2) Position Categorization

Control: The organization:

- a. Assigns a risk designation to all organizational positions;
- b. Establishes screening criteria for individuals filling those positions; and
- c. Reviews and updates position risk designations annually.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address position categorization for the System:

- a. A risk designation to is assigned to all System personnel positions.
- b. Screening criteria are established for individuals filling any positions related to the System.
- c. Risk designation for positions in the System are reviewed and updated annually.

3.8.3 (PS-3) Personnel Screening

Control: The organization:

- a. Screens individuals prior to authorizing access to the information system; and
- b. Rescreens individuals according to agency physical security policy where rescreening is so indicated.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address personnel screening in the System:

- a. Individuals are screened prior to authorizing access to the System
- b. Individuals are rescreened every three (3) years thereafter.

3.8.4 (PS-4) Personnel Termination

Control: The organization, upon termination of individual employment:

- a. Disables information system access immediately or as soon as possible;
- b. Terminates/revokes any authenticators/credentials associated with the individual;
- c. Conducts exit interviews;
- d. Retrieves all security-related organizational information system-related property;
- e. Retains access to organizational information and information systems formerly controlled by terminated individual, and
- f. Notifies IMD as soon as possible.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address personnel termination whenever an individual terminates or is terminated from employment:

- a. Access to System user accounts and any associated system accounts are terminated within one (1) business day.
- b. All authenticators and credentials associated with the individual are revoked immediately
- c. Exit interviews that are conducted that include discussion of information confidentiality, integrity, and the availability of any data associated with the terminated employee.
- d. All security-related information related to the SBIWTP and any property associated with the System is retrieved upon exit.
- e. The SBIWTP retains access to all SBIWTP/IBWC information and System components that were formerly controlled by terminated employee
- f. The SBIWTP system owner and the ISSM are notified within one business day of any personnel termination.

3.8.5 (PS-5) Personnel Transfer

Control: The organization:

- a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
- b. Initiates transfer or reassignment actions within 24 hours;
- c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
- d. Notifies IMD as soon as possible.

Implementation:

System Specific Control

- a. The SBIWTP takes the following actions to address personnel transfer to and away from the System:
- b. An ongoing operational need is reviewed and confirmed for current logical and physical access authorizations to the System and it's associated facilities when individuals are reassigned or transferred to other positions within the SBIWTP/INWC.
- c. All transfer and/or reassignment actions are completed within five (5) business following the formal transfer action unless an exception to complete these tasks is explicitly documented.
- d. Access authorizations are modified as needed to correspond with any changes in operational need due to reassignment or transfer
- e. The SBIWTP system owner and ISSM are notified within one (1) business day of the personnel transfer.

3.8.6 (PS-6) Access Agreements

Control: The organization:

- a. Develops and documents access agreements for organizational information systems;
- b. Reviews and updates the access agreements annually; and
- c. Ensures the individuals requiring access to organizational information and information systems:
 1. Sign appropriate access agreements prior to being granted access; and
 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.

Implementation:

System Specific Control

The SBIWTP takes the following actions to implement access agreements for all employees who access the System:

- a. Access agreements are developed and documented for the System
- b. Access agreements for the System are reviewed and updated annually.

- c. Individuals requiring access to the System are required to sign appropriate access agreements prior to being granted access. Individuals must re-sign any access agreement to maintain access to the System when the access agreement has been updated or it must be re-signed annually if no update was made.

3.8.7 (PS-7) Third-Party Personnel Security

Control: The organization:

- a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
- c. Documents personnel security requirements;
- d. Requires third-party providers to notify IMD of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately and
- e. Monitors provider compliance.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address to address third-party personnel security for the System

- a. Third party personnel security requirements including security roles and responsibilities for third-party providers are established in explicit contract clauses with the SBIWTP and/or IBWC.
- b. Third-party providers are required to comply with the established personnel security policy that is provided by the SBIWTP.
- c. The SBIWTP documents personnel security requirements in its established personnel security policy
- d. Third party providers are required to notify of any personnel transfers or terminations of third-party personnel who possess SBIWTP credentials and/or equipment. This also includes anyone who has System privileges. This must be done within one (1) business day.
- e. Third party provider compliance to the personnel security policy is monitored on a regular basis by performing routine and random checks on any or all of the requirements listed in the SBIWTP personnel security policy.

3.8.8 (PS-8) Personnel Sanctions

Control: The organization:

- a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
- b. Notifies IMD immediately when a formal employee sanction process is initiated, identifying the individual sanctioned and the reason for the sanction.

Implementation:

Inherited Control

The IBWC takes the following actions to address personnel sanctions within the System:

- a. A formal sanctions process is used for individuals failing to comply with established information security policies and procedures. The actual process is handled by the IBWC, an organization that supersedes the SBIWTP.
- b. The SBIWTP system owner and ISSM are notified within a time period defined by the IBWC when a formal employee sanctions process is initiated. The individual being sanctioned is identified and the reason for the sanction is provided.

3.9 (SI) System and Information Integrity

3.9.1 (SI-1) System and Information Integrity Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
- b. Reviews and updates the current:
 1. System and information integrity policy annually; and
 2. System and information integrity procedures annually

Status: This control is currently associated with POA&M #4

Implementation:

System Specific Control

The SBIWTP has taken the following actions to implement a system and information integrity policy and procedures:

- a. A system and information integrity policy have been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The system and information integrity policy are reviewed annually along with its associated implementation procedures.

3.9.2 (SI-2) Flaw Remediation

Control: The organization:

- a. Identifies, reports, and corrects information system flaws;
- b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. Installs security-relevant software and firmware updates as soon as possible of the release of the updates; and
- d. Incorporates flaw remediation into the organizational configuration management process.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address flaw remediation for the System:

- a. Information system flaws are identified, reported, and corrected in accordance with the established policies and procedures.
- b. Software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects before installation.
- c. Security-relevant software and firmware updates are installed in accordance with the system update procedures that have been defined for the System.
- d. Flaw remediation is incorporated into the SBIWTP configuration management process.

SI-2(1) FLAW REMEDIATION | CENTRAL MANAGEMENT

The organization centrally manages the flaw remediation process.

Implementation:

System Specific Control

The SBIWTP centrally manages the flaw remediation process as part of the established CCB process.

SI-2(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

The organization employs automated mechanisms annually to determine the state of information system components with regard to flaw remediation.

Implementation:

System Specific Control

The SBIWTP employs the CDM services to determine the state of System components with regard to flaw remediation.

3.9.3 (SI-3) Malicious Code Protection

Control: The organization:

- a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
- c. Configures malicious code protection mechanisms to:
 1. Perform periodic scans of the information system monthly and real-time scans of files at endpoints or network entry/exit points, as files are downloaded, opened, or executed in accordance with organizational security policy; and
 2. Block malicious code; quarantine malicious code; send alert to the administrator; in response to malicious code detection; and
- d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address malicious code protection on the System:

- a. Malicious code protection mechanisms are employed at the System entry and exit points to detect and eradicate malicious code through the CDM solution.
- b. The malicious code protection mechanisms are updated by the CDM staff whenever new releases are available in accordance with both the GovPlace and the SBIWTP configuration management policy and procedures.
- c. The malicious code protection mechanisms are configured to perform periodic scans of the System continuously. Real-time scans of files are taken from endpoint network entry/exit points as the files are downloaded, opened, or executed in accordance with the SBIWTP System Information and Integrity policy. Malicious code is blocked and/or quarantined as appropriate. Alert are sent to the CDM staff members in response to a malicious code being detected.
- d. The receipt of false positives is addressed during malicious code detection and eradication. The potential impact on the availability of the System is also evaluated.

SI-3(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages malicious code protection mechanisms.

Implementation:

System Specific Control

The SBIWTP centrally manages malicious code protection mechanisms by deploying them on the CDM server.

SI-3(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

The information system automatically updates malicious code protection mechanisms.

Implementation:

System Specific Control

3.9.4 (SI-4) Information System Monitoring Tools and Techniques

Control: The organization:

- a. Monitors the information system to detect:
 1. Attacks and indicators of potential attacks in accordance with CDM monitoring objectives]; and
 2. Unauthorized local, network, and remote connections;
- b. Identifies unauthorized use of the information system through CDM organization-defined techniques and methods;
- c. Deploys monitoring devices:
 1. Strategically within the information system to collect organization-determined essential information; and
 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
- f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
- g. Provides information system monitoring information to SBITWP operations and SCADA maintenance contractors as needed.

Implementation:

System Specific Control

The SBIWTP takes the following actions to implement monitoring tools and techniques on the System:

- a. The System is monitored by the CDM solution to detect attacks and indicators of potential attacks in accordance with the defined monitoring objectives in the System policies and procedures. Additionally, unauthorized local, network and remote connections are also detected.
- b. Unauthorized use of the System is detected through the defined audit policy and its associated procedures.
- c. Monitoring devices are deployed strategically within the System using the CDM solution to collect essential information. They are deployed at ad hoc locations within the system to track specific types of transactions of interest to the SBIWTP. Information that is obtained from intrusion-monitoring tools is protected from unauthorized access, modification, and deletion;
- d. The information obtained from intrusion-monitoring tools is protected from unauthorized access, modification, and deletion;
- e. The level of System monitoring activity is heightened whenever there is an indication of increased risk to SBIWTP operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
- f. Legal opinion is obtained regarding any system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
- g. System monitoring information is forwarded to the CDM staff members and the ISSM as needed on a monthly basis.

SI-4(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

The organization employs automated tools to support near real-time analysis of events.

Implementation:

System Specific Control

The SBIWTP employs automated tools to support near real-time analysis of events through the CDM solution.

SI-4(4) *INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*

The information system monitors inbound and outbound communications traffic annually for unusual or unauthorized activities or conditions.

Implementation:

System Specific Control

The SBIWTP monitors inbound and outbound communications traffic on the System continuously for unusual or unauthorized activities or conditions using the CDM solution.

SI-4(5) *INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*

The information system alerts SBITWP operations and SCADA maintenance contractors when the following indications of compromise or potential compromise occur:

Implementation:

System Specific Control

The System alerts the CDM staff when any indications of compromise or potential compromise occur.

3.9.5 (SI-5) Security Alerts and Advisories

Control: The organization:

- a. Receives information system security alerts, advisories, and directives from the IMD on an ongoing basis;
- b. Generates internal security alerts, advisories, and directives as deemed necessary;
- c. Disseminates security alerts, advisories, and directives to: SBIWTP operations and SCADA system maintenance contractors, and
- d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address security alerts and advisories on the System:

- a. Information system security alerts, advisories, and directives are received from the defined external organizations on an ongoing basis that is monitored by the CDM staff.
- b. Internal security alerts, advisories, and directives are generated as deemed necessary.
- c. Security alerts, advisories, and directives to are disseminated to all CDM staff
- d. Security directives are implemented in accordance with established time frames.

SI-5(1) *SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms using the CDM solution to make security alert and advisory information regarding the System are available throughout the SBIWTP.

3.9.6 (SI-6) Security Functionality Verification

Control: The information system:

- a. Verifies the correct operation of security functions;
- b. Performs this verification upon command by user with appropriate privileges;
- c. Notifies SBITWP operations and SCADA maintenance contractors of failed security verification tests; and
- d. Shuts the information system down; restarts the information system when anomalies are discovered.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address security functionality verification on the System:

- a. The correct operations of the CDM tools are verified through regular testing. Additionally, username and password distributions for the HMIs are validated on an annual basis
- b. Verification is performed on the SBIWTP defined transitional states upon command by a user with appropriate privilege. These verifications are conducted annually.
- c. The System Owner and ISSM are notified of any failed security verification tests.
- d. The proper alerts are generated when any anomalies are discovered.

3.9.7 (SI-7) Software and Information Integrity

Control: The organization employs integrity verification tools to detect unauthorized changes to software, or firmware.

Implementation:

System Specific Control

The SBIWTP employs integrity verification tools to detect unauthorized changes to any System software, firmware, and information by deploying the CDM solution.

SI-7(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

The information system performs an integrity check of software or firmware, and at startup; or security-relevant events.

Implementation:

System Specific Control

The System regularly performs an integrity check of all software, firmware, and information. These are done monthly at a minimum.

SI-7(2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

The organization employs automated tools that provide notification to SBITWP operations and SCADA maintenance contractors upon discovering discrepancies during integrity verification.

Implementation:

System Specific Control

The SBIWTP employs automated tools through the CDM solution that provide notification to the CDM staff, the System Owner, and the ISSM upon discovering discrepancies during integrity verification.

SI-7(5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

The information system automatically *shuts the information system down* and implements security safeguards when integrity violations are discovered.

Implementation:

System Specific Control

The System implements alerting features through the CDM solution as a security safeguard when integrity violations are discovered.

SI-7(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

The organization incorporates the detection of unauthorized *changes to the information system*.

Implementation:

System Specific Control

The SBIWTP incorporates the detection of unauthorized changes to the System into the incident response capability.

SI-7(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*

The organization:

- (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and**
- (b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.**

Implementation:

System Specific Control

The SBIWTP takes the following actions to address binary or machine executable code on the System:

- a. The use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code is strictly prohibited.
- b. Exceptions to the source code requirement are provided only for compelling mission/operational requirements and with the approval of the System authorizing official.

3.9.8 (SI-8) Spam Protection

Control: The organization:

- a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
- b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Implementation:

Not Applicable

Spam protection mechanisms are not needed due to SCADA devices, not having access to the internet or email.

SI-8(1) *SPAM PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages spam protection mechanisms.

Implementation:

System Specific Control

The SBIWTP centrally manages spam protection mechanisms using the CDM solution.

SI-8(2) *SPAM PROTECTION | AUTOMATIC UPDATES*

The information system automatically updates spam protection mechanisms.

Implementation:

Inherited Control

The SBIWTP relies on the CDM solution to update the spam protection mechanisms on the System.

3.9.9 (SI-10) Information Accuracy, Completeness, Validity, and Authenticity

Control: The information system checks the validity of information inputs

Implementation:

System Specific Control

The System checks the validity of all information that is input by the user using the Ignition software that is deployed on the HMIs.

3.9.10 (SI-11) Error Handling

Control: The information system:

- a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- b. Reveals error messages only to SBITWP operations and SCADA maintenance contractors

Implementation:

System Specific Control

The SBIWTP takes the following actions to address error handling on the System:

- a. Error messages are generated through SCADA alarm messages. These provide the information necessary for corrective actions without revealing information that could be exploited by adversaries.
- b. Error messages are revealed only to the following persons with the following roles:
 - i. The System Owner
 - ii. The System ISSM
 - iii. The assigned SCADA Operators

3.9.11 (SI-12) Information Output Handling and Retention

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementation:

System Specific Control

The SBIWTP handles and retains information within the System and information output from the System in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

3.9.12 (SI-16) Memory Protection

Control: The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution

Implementation:

System Specific Control

The System implements the appropriate security safeguards to protect its memory from unauthorized code execution.

4 TECHNICAL CONTROLS

4.1 (AC) Access Control

4.1.1 (AC-1) Access Control Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors:
 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
- b. Reviews and updates the current:
 1. Access control policy annually; and

2. Access control procedures annually.

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement access control policy and procedures:

- a. An access control policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the access control policy; and the associated security controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The access control policy is reviewed annually along with its associated implementation procedures.

4.1.2 (AC-2) Account Management

Control: The organization:

- a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: IMD administrators;
- b. Assigns account managers for information system accounts;
- c. Establishes conditions for group and role membership;
- d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e. Requires approvals by SBITWP operations and SCADA maintenance contractors for requests to create information system accounts;
- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with IMD defined procedures;
- g. Monitors the use of information system accounts;
- h. Notifies account managers:
 1. When accounts are no longer required;
 2. When users are terminated or transferred; and
 3. When individual information system usage or need-to-know changes;
- i. Authorizes access to the information system based on:
 1. A valid access authorization;
 2. Intended system usage; and
 3. Other attributes as required by the organization or associated missions/business functions;
- j. Reviews accounts for compliance with account management requirements annually; and
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Implementation:

System Specific Control

SBIWTP has taken the following actions to perform account management:

- a. System accounts have been identified to support SBIWTP missions/business functions: unprivileged user accounts, privileged admin accounts, and non-interactive service accounts.
- b. Account managers are assigned for System accounts;
- c. Conditions for group and role membership are established
- d. Authorized users of the System are specified and group/role membership, and access authorizations (i.e., privileges) and other attributes (as required) are specified for each account.
- e. Approvals are required by the System Owner and ISSM for requests to create accounts on the System.
- f. System accounts on the System are created, enabled, modified, disabled, and removed in accordance with SCADA Network standard operating procedures;
- g. The use of SCADA Network accounts is monitored continuously
- h. Account managers are notified under the following conditions when accounts are no longer required. They are also notified upon termination/transfer and when individual's usage or need-to-know changes;

- i. Access authorizations to the System are based on a valid access authorization; the intended system usage, and any other attributes as required by the SBIWTP or associated missions/business functions;
- j. Accounts are reviewed for compliance with the established account management requirements on a monthly basis.
- k. Shared account credentials are not deployed on the System.

AC-2(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

The organization employs automated mechanisms to support the management of information system accounts.

Implementation:

System Specific Control

The SBIWTP employs automated mechanisms in Active Directory and the Ignition software to support the management of information system accounts.

AC-2(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

The information system automatically *disables* temporary and emergency accounts after 30 days of inactivity.

Implementation:

System Specific Control

The SBIWTP SCADA Network automatically disables temporary and emergency accounts after a time period matching the mission/business justification given with the account creation request, and/or as part of the monthly account review.

AC-2(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

The information system automatically disables inactive accounts after 30 days of inactivity.

Implementation:

System Specific Control

The System automatically disables inactive accounts after thirty (30) days of inactivity.

AC-2(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies SBITWP operations and SCADA maintenance contractors .

Implementation:

System Specific Control

The System automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies SBIWTP security operations staff.

AC-2(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

The organization requires that users log out after 30 minutes of inactivity.

Implementation:

System Specific Control

The System automatically logs users out when a session is inactive for more than one (1) hour.

AC-2(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS

The information system enforces role based usage conditions for users, privileged admin and non-interactive service accounts.

Implementation:

System Specific Control

The SBIWTP SCADA Network enforces exclusive separation between normal user, privileged admin, and non-interactive service accounts with no user account role overlap.

AC-2(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE

The organization:

- (a) Monitors information system accounts for [Assignment: organization-defined atypical usage]; and**
- (b) Reports atypical usage of information system accounts to SBITWP operations and SCADA maintenance contractors .**

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement account usage monitoring:

- a. The System accounts are monitored for unauthorized activity
- b. A typical usage of System accounts is reported to SBIWTP security operations staff.

AC-2(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

The organization disables accounts of users possessing a significant risk within [Assignment: organization-defined time period] of the discovery of the risk.

Implementation:

System Specific Control

The SBIWTP disables user accounts that are deemed to present a significant risk within twenty-four (24) hours of discovery of the risk.

4.1.3 (AC-3) Access Enforcement

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Implementation:

System Specific Control

The System enforces approved authorizations for logical access to its information and system resources in accordance with the System access control policy.

AC-3(2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION

The information system enforces dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].

Implementation:

System Specific Control

The System enforces dual authentication for all access to the System using Personal Identity Verification (PIV) credentials

4.1.4 (AC-4) Information Flow Enforcement

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

Implementation:

System Specific Control

The System enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on Access Control Lists (ACLs).

4.1.5 (AC-5) Separation of Duties

Control: The organization:

- a. Separates *[Assignment: organization-defined duties of individuals]*;
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address separation of duties on the System:

- a. The System has users that are separated into four (4) working groups:
 - i. Area Operations Manager
 - ii. Administrator
 - iii. Plant Operator
 - iv. Field Operator
- b. Separation of duties is documented by individuals in defined access control lists
- c. The System access authorizations are defined in the SBIWTP Access Control Policy

4.1.6 (AC-6) Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Implementation:

System Specific Control

The System employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with SBIWTP missions and business functions. This concept is enforced by using the user account groups defined in Section 4.1.5

AC-6(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to *[Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]*.

Implementation:

System Specific Control

SBIWTP explicitly authorizes access to privileged administrative account functions and security-relevant information.

AC-6(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to *[Assignment: organization-defined security functions or security-relevant information]*, use non-privileged accounts or roles when accessing non-security functions.

Implementation:

System Specific Control

SBIWTP requires that users of System accounts, or roles, with access to mission-critical information and security-related functionality, use non-privileged accounts or roles when accessing non-security functions.

AC-6(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

The organization authorizes network access to *[Assignment: organization-defined privileged commands]* only for *[Assignment: organization-defined compelling operational needs]* and documents the rationale for such access in the security plan for the information system.

Implementation:

System Specific Control

SBIWTP authorizes network access to privileged functions of the System only for strict administrative, operational, and security needs; with accompanying documentation of the rationale for such access in the SCADA Network security plan.

AC-6(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to SBITWP operations and SCADA maintenance contractors .

Implementation:

System Specific Control

SBIWTP restricts privileged accounts on the System to system administrators and the Area Operations Manager.

AC-6(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Implementation:

System Specific Control

The System audits the execution of privileged functions on the system through the use of a SYSLOG server.

AC-6(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Implementation:

System Specific Control

The System prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

4.1.7 (AC-7) Unsuccessful Login Attempts

Control: The information system:

- a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid log-on attempts by a user during a [*Assignment: organization-defined time period*]; and
- b. Automatically [*Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next log-on prompt according to [Assignment: organization-defined delay algorithm]*] when the maximum number of unsuccessful attempts is exceeded.

Implementation:

System Specific Control

The System takes the following actions to address unsuccessful login attempts on the System:

- a. Enforces a limit of five (5) consecutive invalid log-on attempts by a user during a 5-minute time period; and
- b. Automatically delays next log-on prompt for fifteen (15) minutes when the maximum number of unsuccessful attempts is exceeded.

4.1.8 (AC-8) System Use Notification

Control: The information system:

- a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;
 2. Information system usage may be monitored, recorded, and subject to audit;
 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
 4. Use of the information system indicates consent to monitoring and recording;
- b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
- c. For publicly accessible systems:
1. Displays system use information [Assignment: organization-defined conditions], before granting further access;
 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
 3. Includes a description of the authorized users of the system.

Implementation:

System Specific Control

The System:

- a. Displays to users a system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
 - i. Users are accessing a U.S. Government information system;
 - ii. Information system usage may be monitored, recorded, and subject to audit;
 - iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
 - iv. Use of the information system indicates consent to monitoring and recording;
- b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
- c. For publicly accessible systems:
 - i. Displays system use requirements, before granting further access;
 - ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
 - iii. Includes a description of the authorized users of the system.

4.1.9 (AC-10) Concurrent Session Control

Control: The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

Implementation:

System Specific Control

The System does not allow concurrent sessions on any of its devices.

4.1.10 (AC-11) Session Lock

Control: The information system:

- a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Implementation:

System Specific Control

The System:

- a. Further access to the system is prevented by initiating a session lock after five (5) minutes of inactivity or upon receiving a request from a user; and

- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11(1) *SESSION LOCK | PATTERN-HIDING DISPLAYS*

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Implementation:

System Specific Control

The System conceals, via the session lock, information previously visible on the display with a publicly viewable image.

4.1.11 (AC-12) Session Termination

Control: The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Implementation:

System Specific Control

The System automatically terminates a user session after it has been inactive for 4 hours.

4.1.12 (AC-14) Permitted Actions w/o Identification or Authentication

Control: The organization:

- a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
- b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Implementation:

System Specific Control

SBIWTP has taken the following actions to restrict actions permitted without identification and authentication:

- a. Identified the minimum actions that can be performed on the information system without identification or authentication consistent with SBIWTP missions/business functions, and risk tolerance; and
- b. Documented and provides supporting rationale in the security plan for the SCADA Network, user actions not requiring identification or authentication.

4.1.13 (AC-17) Remote Access

Control: The organization:

- a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
- b. Authorizes remote access to the information system prior to allowing such connections.

Status: This control is currently associated with POA&M #6

Implementation:

System Specific Control

SBIWTP has taken the following actions to restrict remote access:

- a. Established and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
- b. Authorized remote access to the information system prior to allowing such connections.

AC-17(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

Implementation:

System Specific Control

The System monitors and controls remote access methods. Only specific individuals can remote into the System.

AC-17(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Implementation:

System Specific Control

The System implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

Implementation:

System Specific Control

The System routes all remote accesses through one central managed network access control point.

AC-17(4) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS

The organization:

- (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and**
- (b) Documents the rationale for such access in the security plan for the information system.**

Implementation:

System Specific Control

SBIWTP has taken the following actions to restrict execution of privileged commands through remote access:

- a. Authorized the execution of privileged commands and access to security-relevant information via remote access only for approved system administrative activities; and
- b. Documented the rationale for such access in the security plan for the information system.

4.1.14 (AC-18) Wireless Access Restrictions

Control: The organization:

- a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
- b. Authorizes wireless access to the information system prior to allowing such connections.

Implementation:

Not Applicable

Wireless Access Points are not available for the SBIWTP SCADA System.

AC-18(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

Implementation:

Not Applicable

Wireless Access Points are not available for the SBIWTP SCADA System.

AC-18(4) *WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Implementation:

Not Applicable

Wireless Access Points are not available for the SBIWTP SCADA System.

AC-18(5) *WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Implementation:

System Specific Control

The SBIWTP selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of SBIWTP-controlled boundaries.

4.1.15 (AC-19) Access Control for Portable and Mobile Devices

Control: The organization:

- a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
- b. Authorizes the connection of mobile devices to organizational information systems.

Implementation:

System Specific Control

The SBIWTP takes the following actions to address access control for portable and mobile devices:

- a. Usage restrictions, configuration requirements, connection requirements, and implementation guidance are established for SBIWTP-controlled mobile devices
- b. All connection of mobile devices is authorized to the System.

AC-19(5) *ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*

The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].

Implementation:

Not Applicable

The SCADA network does not allow the use of mobile devices.

4.1.16 (AC-20) Use of External Information Systems

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- a. Access the information system from external information systems; and
- b. Process, store, or transmit organization-controlled information using external information systems.

Implementation:

System Specific Control

SBIWTP establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- a. Access the System from external information systems; and
- b. Process, store, or transmit organization-controlled information using external information systems.

AC-20(1) *USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

- (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or**
- (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.**

Implementation:

System Specific Control

SBIWTP permits authorized individuals to use an external information system to access the SCADA Network or to process, store, or transmit organization-controlled information only when the organization:

- a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
- b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-20(2) *USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Implementation:

System Specific Control

The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

4.1.17 (AC-21) Information Sharing

Control: The organization:

- a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
- b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

Implementation:

System Specific Control

- a. The SBIWTP takes the following actions to address information sharing on the System:
Information sharing is facilitated by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for SBIWTP sharing purposes
- b. Security guidance is employed to assist users in making information sharing/collaboration decisions.

4.1.18 (AC-22) Publicly Accessible Content

Control: The organization:

- a. Designates individuals authorized to post information onto a publicly accessible information system;
- b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
- d. Reviews the content on the publicly accessible information system for nonpublic information annually and removes such information, if discovered.

Implementation:

System Specific Control

SBIWTP has taken the following actions to secure publicly accessible content:

- a. Designated individuals authorized to post information onto a publicly accessible information system;
- b. Routinely trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Periodically reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
- d. Periodically reviews the content on the publicly accessible information system for nonpublic information monthly, and removes such information, if discovered.

4.2 (AU) Audit and Accountability

4.2.1 (AU-1) Audit and Accountability Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
- b. Reviews and updates the current:
 1. Audit and accountability policy annually; and
 2. Audit and accountability procedures annually.

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement audit and accountability policy and procedures:

- a. An audit and accountability policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the audit and accountability policy; and the associated security controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The audit and accountability policy are reviewed annually along with its associated implementation procedures.

4.2.2 (AU-2) Auditable Events

Control: The organization:

- a. Determines that the information system is capable of auditing the following events:
[Assignment: organization-defined auditable events];
- b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determines that the following events are to be audited within the information system:
[Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

Implementation:

System Specific Control

SBIWTP has taken the following actions to define auditable events:

- a. Determined that the information system is capable of auditing the following events:
 - i. Network Events,
 - ii. Infrastructure Events,
 - iii. Operating System Events,
 - iv. Application Events,
 - v. Continuous Monitoring Events;
- b. Coordinated the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- c. Provided a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determined that the following events are to be audited within the information system:
 - i. Network Events,
 - ii. Infrastructure Events,
 - iii. Operating System Events,
 - iv. Application Events,
 - v. Continuous Monitoring Events;

AU-2(3) AUDIT EVENTS | REVIEWS AND UPDATES

The organization reviews and updates the audited events annually.

Implementation:

System Specific Control

SBIWTP reviews and updates the audited events when significant changes to the System occur and when the Authority to Operate status is scheduled for renewal.

4.2.3 (AU-3) Content of Audit Records

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Implementation:

System Specific Control

The System generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

AU-3(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

Implementation:

System Specific Control

The System generates audit records containing no other significant information beyond the requirements established by AU-3.

AU-3(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].

Implementation:

System Specific Control

The System provides centralized management and configuration of the content to be captured in audit records generated by network, infrastructure, operating system, application, and monitoring level components.

4.2.4 (AU-4) Audit Storage Capacity

Control: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

Implementation:

System Specific Control

SBIWTP allocates audit record storage capacity in accordance with audit record storage requirements.

4.2.5 (AU-5) Response to Audit Processing Failures

Control: The information system:

- a. Alerts SBITWP operations and SCADA maintenance contractors in the event of an audit processing failure; and
- b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

AU-5(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY

The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.

Implementation:

System Specific Control

The System:

- a. Alerts the SBIWTP security operations staff in the event of an audit processing failure; and
- b. Takes the no other additional actions.

AU-5(2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS

The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].

Implementation:

System Specific Control

The information system provides an alert in near-real-time to SBIWTP security operations staff when audit failure events occur.

4.2.6 (AU-6) Audit Monitoring, Analysis, and Reporting

Control: The organization:

- a. Reviews and analyzes information system audit records annually for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
- b. Reports findings to SBITWP operations and SCADA maintenance contractors .

Implementation:

System Specific Control

The SBIWTP security operations staff review and analyze information system audit records for the System at regular intervals for indications of inappropriate or unusual activity; then report findings to the Information System Security Manager and supporting staff.

AU-6(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Implementation:

System Specific Control

The System employs automated mechanisms to integrate audit review, analysis, and reporting processes to support the SBIWTP continuous monitoring and SBIWTP incident response processes.

AU-6(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Implementation:

System Specific Control

SBIWTP analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AU-6(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES

The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

Implementation:

System Specific Control

The SBIWTP security operations staff integrates analysis of audit records with analysis of the data provided by the CDM solution covering vulnerability scanning, configuration compliance, and performance statistics; all to further enhance the ability to identify inappropriate or unusual activity.

AU-6(6) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Implementation:

System Specific Control

The SBIWTP security operations staff correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

4.2.7 (AU-7) Audit Reduction and Report Generation

Control: The information system provides an audit reduction and reports generation capability that:

- a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
- b. Does not alter the original content or time ordering of audit records.

Implementation:

System Specific Control

The System provides an audit reduction and reports generation capability that:

- a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
- b. Does not alter the original content or time ordering of audit records.

AU-7(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

Implementation:

System Specific Control

The System provides the capability to process audit records for events of interest based on username, machine name, IP address, and other fields which can tie system activity back to an identity.

4.2.8 (AU-8) Time Stamps

Control: The information system:

- a. Uses internal system clocks to generate time stamps for audit records; and
- b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

Implementation:

System Specific Control

The System:

- a. Uses internal system clocks to generate time stamps for audit records; and
- b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) and Greenwich Mean Time (GMT), meeting Network Time Protocol (NTP) standards.

AU-8(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system:

- (a) Compares the internal information system clocks annually with [Assignment: organization-defined authoritative time source]; and**
- (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].**

Implementation:

System Specific Control

The System:

- a. Compares the internal information system clocks periodically with a secure Network Time Protocol (NTP) server; and
- b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than allowable for stable operation of the system.

4.2.9 (AU-9) Protection of Audit Information

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Implementation:

System Specific Control

The System protects audit information and audit tools from unauthorized access, modification, and deletion.

AU-9(2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

The information system backs up audit records annually onto a physically different system or system component other than the system or component being audited.

Implementation:

System Specific Control

The System backs up audit records periodically onto a physically different system or system component other than the system or component being audited.

AU-9(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Implementation:

System Specific Control

The System implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

AU-9(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

The organization authorizes access to management of audit functionality to only

**[Assignment: organization
-defined subset of privileged users].**

Implementation:

System Specific Control

SBIWTP authorizes access to management of audit functionality to only necessary users who are either managing the auditing capability or who have a need-to-know the information.

4.2.10 (AU-10) Non-Repudiation

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

Implementation:

System Specific Control

The System protects against an individual (or process acting on behalf of an individual) falsely denying having performed audited activities which are tied to their digital identity.

4.2.11 (AU-11) Audit Record Retention

Control: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Implementation:

System Specific Control

SBIWTP retains audit records for a time period consistent with records retention policy, to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

4.2.12 (AU-12) Audit Generation

Control: The information system:

- a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];
- b. Allows SBITWP operations and SCADA maintenance contractors to select which auditable events are to be audited by specific components of the information system; and
- c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Implementation:

System Specific Control

The System:

- a. Provides audit record generation capability for the auditable events defined in AU-2 a. at the network, infrastructure, operating system, application, and monitoring levels;
- b. Allows SBIWTP management and security operations staff to select which auditable events are to be audited by specific components of the information system; and
- c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

AU-12(1) AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL

The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

Implementation:

System Specific Control

The System compiles audit records from the network, infrastructure, operating system, application, and monitoring levels into a system-wide (logical or physical) audit trail that is time-correlated to within an acceptable level of accuracy to ensure the integrity of audit records.

AU-12(3) AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

The information system provides the capability for IMD to change the auditing to be performed on SCADA system components based on changes annually

Implementation:

System Specific Control

The System provides the capability for SBIWTP management and security operations staff to change the auditing to be performed on the network, infrastructure, operating system, application, and monitoring levels based on operational changes to the system within a short time period.

4.3 (IA) Identification and Authentication

4.3.1 (IA-1) Identification and Authentication Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
- b. Reviews and updates the current:
 1. Identification and authentication policy annually; and
 2. Identification and authentication procedures annually.

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement identification and authentication policy and procedures:

- a. An identification and authentication policy has been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the identification and authentication policy; and the associated system and the identification and authentication controls. These policies and procedures have been distributed to the System Owner and the ISSM.
- b. The identification and authentication policy is reviewed annually along with the associated implementation procedures.

4.3.2 (IA-2) User Identification and Authentication

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Implementation:

System Specific Control

The System uniquely identifies and authenticates SBIWTP users and processes acting on behalf of SBIWTP users.

IA-2(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to privileged accounts.

Implementation:

System Specific Control

The System implements multifactor authentication for network access to privileged accounts.

IA-2(2) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to non-privileged accounts.

Implementation:

System Specific Control

The system implements multifactor authentication for network access to non-privileged accounts.

IA-2(3) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for local access to privileged accounts.

Implementation:

System Specific Control

The System implements multifactor authentication for local access to privileged accounts.

IA-2(4) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for local access to non-privileged accounts.

Implementation:

System Specific Control

The SBIWTP SCADA Network implements multifactor authentication for local access to non-privileged accounts.

IA-2(8) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Implementation:

System Specific Control

The SBIWTP SCADA Network implements replay-resistant authentication mechanisms for network access to privileged accounts.

IA-2(9) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Implementation:

System Specific Control

The SBIWTP SCADA Network implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

IA-2(11) *IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: the organization-defined strength of mechanism requirements].

Implementation:

System Specific Control

The System implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets FIPS 201 requirements.

IA-2(12) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Status: This control is currently associated with POA&M #5

Implementation:

System Specific Control

The system will be built to accept PIV cards. Currently, PIV cards are not operational and the users only access the system with username and password.

4.3.3 (IA-3) Device Identification and Authentication

Control: The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

Implementation:

System Specific Control

The System uniquely identifies and authenticates approved, trusted, and secure devices before establishing a network connection.

4.3.4 (IA-4) Identifier Management

Control: The organization manages information system identifiers by:

- a. Receiving authorization from SBITWP operations and SCADA maintenance contractors to assign an individual, group, role, or device identifier;
- b. Selecting an identifier that identifies an individual, group, role, or device;
- c. Assigning the identifier to the intended individual, group, role, or device;
- d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and
- e. Disabling the identifier after [Assignment: the organization-defined time period of inactivity].

Implementation:

System Specific Control

SBIWTP takes the following actions to manage the SCADA Network identifiers:

- a. Receives authorization from the System Owner or their designated appointee to assign an individual, group, role, or device identifier;
- b. Selects an identifier that identifies an individual, group, role, or device;
- c. Assigns the identifier to the intended individual, group, role, or device;
- d. Prevents reuse of identifiers for after expiration; and
- e. Disables the identifier after time inactivity limit.

4.3.5 (IA-5) Authenticator Management

Control: The organization manages information system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators prior to information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- g. Changing/refreshing authenticators within 30 minutes;
- h. Protecting authenticator content from unauthorized disclosure and modification;
- i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- j. Changing authenticators for group/role accounts when membership to those accounts changes.

Implementation:

System Specific Control

SBIWTP takes the following actions to manage the SCADA Network authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators prior to information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

- g. Changing/refreshing authenticators when authenticators are stolen, lost, damaged, or have exceeded their maximum lifetime;
- h. Protecting authenticator content from unauthorized disclosure and modification;
- i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- j. Changing authenticators for group/role accounts when membership to those accounts changes.

IA-5(1) *AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*

The information system, for password-based authentication:

- (a) Enforces minimum password complexity of case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type;**
- (b) Enforces at least the following number of changed characters when new passwords are created: 1;**
- (c) Stores and transmits only cryptographically protected passwords;**
- (d) Enforces password minimum and maximum lifetime restrictions of 6 (six) numbers for lifetime minimum, lifetime maximum];**
- (e) Prohibits password reuse for 6 (six) generations; and**
- (f) Allows the use of a temporary password for system log-ons with an immediate change to a permanent password.**

Implementation:

System Specific Control

The System, for password-based authentication:

- a. Enforces minimum password complexity of at least 12 characters, to include at least one numeric, one uppercase, one lowercase, one non-alphanumeric symbol;
- b. Enforces at least the following number of changed characters when new passwords are created:
1
- c. Stores and transmits only cryptographically protected passwords;
- d. Enforces password minimum and maximum lifetime restrictions of 60 days;
- e. Prohibits password reuse for 10 generations; and
- f. Allows the use of a temporary password for system log-ons with an immediate change to a permanent password.

4.3.6 (IA-6) Authenticator Feedback

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Implementation:

System Specific Control

The System obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

4.3.7 (IA-7) Cryptographic Module Authentication

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Implementation:

System Specific Control

The System implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable state laws, federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

4.3.8 (IA-8) Cryptographic Module Authentication

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Implementation:

System Specific Control

The System uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

IA-8(1) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Implementation:

System Specific Control

The System accepts and electronically verifies CAC credentials from other federal and state agencies.

IA-8(2) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*

The information system accepts only FICAM-approved third-party credentials.

Implementation:

System Specific Control

The System accepts only FICAM-approved third-party credentials.

IA-8(3) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS*

The organization employs only FICAM-approved information system components within the SCADA system to accept third-party credentials.

Implementation:

System Specific Control

SBIWTP employs only FICAM-approved information system components in the centralized authentication solution to accept third-party credentials.

IA-8(4) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES*

The information system conforms to FICAM-issued profiles.

Implementation:

System Specific Control

The System conforms to FICAM-issued profiles.

4.4 (SC) System and Communications Protection

4.4.1 (SC-1) System and Communications Protection Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to SBITWP operations and SCADA maintenance contractors :
 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
- b. Reviews and updates the current:
 1. System and communications protection policy annually; and
 2. System and communications protection procedures annually.

Status: This control is currently associated with POA&M #7

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement system and communications protection policy and procedures:

- a. A system and communications protection policy have been developed to address, purpose, scope, roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance. Procedures have also been developed to facilitate the implementation of the system and communications protection policy; and the associated system and the system and communications protection controls. These policies and procedures have been distributed to the System owner and the ISSM.
- b. The system and communications protection policy are reviewed annually along with the associated implementation procedures.

4.4.2 (SC-2) Application Partitioning

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Implementation:

System Specific Control

The System separates user functionality (including user interface services) from information system management functionality.

4.4.3 (SC-3) Security Function Isolation

Control: The information system isolates security functions from non-security functions.

Implementation:

System Specific Control

The System isolates security functions from non-security functions.

4.4.4 (SC-4) Information Remnants

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Implementation:

System Specific Control

The System prevents unauthorized and unintended information transfer via shared system resources.

4.4.5 (SC-5) Denial of Service Protection

Control: The information system protects against or limits the effects of the following types of denial of service attacks: by employing CDM security safeguards.

Implementation:

System Specific Control

The System protects against and limits the effects of distributed and single-origin denial of service attacks by employing CDM tools.

4.4.6 (SC-7) Boundary Protection

Control: The information system:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
- c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Implementation:

System Specific Control

The System:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
- c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the CDM-enabled security architecture.

SC-7(3) BOUNDARY PROTECTION | ACCESS POINTS

The organization limits the number of external network connections to the information system.

Implementation:

System Specific Control

SBIWTP limits the number of external network connections to the information system.

SC-7(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

The organization:

- (a) Implements a managed interface for each external telecommunication service;**
- (b) Establishes a traffic flow policy for each managed interface;**
- (c) Protects the confidentiality and integrity of the information being transmitted across each interface;**
- (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and**
- (e) Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.**

Implementation:

System Specific Control

SBIWTP has taken the following actions to secure external telecommunications services:

- a. Implemented a managed interface for each external telecommunication service;
- b. Established a traffic flow policy for each managed interface;
- c. Protects the confidentiality and integrity of the information being transmitted across each interface;
- d. Documented each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- e. Reviews exceptions to the traffic flow policy when mission/business need duration expires and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Implementation:

System Specific Control

The System at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

SC-7(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Implementation:

System Specific Control

The System, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

SC-7(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

The information system routes *communications traffic* to internal *networks only* through authenticated proxy servers at managed interfaces.

Implementation:

System Specific Control

The System routes internal web traffic to the outside through authenticated proxy servers at managed interfaces.

SC-7(18) BOUNDARY PROTECTION | FAIL SECURE

The information system fails securely in the event of an operational failure of a boundary protection device.

Implementation:

System Specific Control

The System fails securely in the event of an operational failure of a boundary protection device.

SC-7(21) BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS

The organization employs boundary protection mechanisms to separate *SCADA system components and/or business functions*.

Implementation:

System Specific Control

SBIWTP employs boundary protection mechanisms to separate SCADA network system components supporting missions and business functions.

4.4.7 (SC-8) Transmission Confidentiality and Integrity

Control: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

Implementation:

System Specific Control

The System protects the confidentiality and integrity of transmitted information.

SC-8(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

Implementation:

System Specific Control

The System implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by mitigating controls.

4.4.8 (SC-10) Network Disconnect

Control: The information system terminates the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

Implementation:

System Specific Control

The System terminates the network connection associated with a communications session at the end of the session or after 5 minutes of inactivity

4.4.9 (SC-12) Cryptographic Key Establishment and Management

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with IMD requirements for key generation, distribution, storage, access, and destruction.

Implementation:

Not Applicable

PKI is not used in the SCADA environment.

SC-12(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*

The organization maintains the availability of information in the event of the loss of cryptographic keys by users.

Implementation:

System Specific Control

SBIWTP maintains the availability of information in the event of the loss of cryptographic keys by users.

4.4.10 (SC-13) Use of Cryptography

Control: The information system implements cryptography required in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Implementation:

System Specific Control

The System defined cryptographic uses and the type of cryptography required for each use, in accordance with applicable state laws, federal laws, Executive Orders, directives, policies, regulations, and standards.

4.4.11 (SC-15) Collaborative Computing

Control: The information system:

- a. Prohibits remote activation of collaborative computing; and
- b. Provides an explicit indication of use to users physically present at the devices.

Implementation:

System Specific Control

The System:

- a. Prohibits remote activation of collaborative computing devices unless otherwise approved by the system owner; and
- b. Provides an explicit indication of use to users physically present at the devices.

4.4.12 (SC-17) Public Key Infrastructure Certificates

Control: The organization issues public key certificates under IMD certificate policy and obtains public key certificates from an approved service provider.

Implementation:

Not Applicable

PKI is not utilized for the SBIWTP SCADA System.

(SC-18) Mobile Code

Control: The organization:

- a. Defines acceptable and unacceptable mobile code and mobile code technologies;
- b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- c. Authorizes, monitors, and controls the use of mobile code within the information system.

Implementation:

System Specific Control

SBIWTP has taken the following actions to secure mobile code:

- a. Defined acceptable and unacceptable mobile code and mobile code technologies;
- b. Established usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- c. Authorizes, monitors and controls the use of mobile code within the SCADA Network.

4.4.13 (SC-19) Voice Over Internet Protocol

Control: The organization:

- a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
- b. Authorizes, monitors, and controls the use of VoIP within the information system.

Implementation:

System Specific Control

SBIWTP has taken the following actions to secure Voice over IP Protocol:

- a. Established usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
- b. Authorizes, monitors and controls the use of VoIP within the information system.

4.4.14 (SC-20) Secure Name/Address Resolution Service (Authoritative Source)

Control: The information system:

- a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
- b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Implementation:

System Specific Control

The System:

- a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
- b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

4.4.15 (SC-21) Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Implementation:

System Specific Control

The System requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

4.4.16 (SC-22) Architecture and Provisioning for Name/Address Resolution Service

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Implementation:

System Specific Control

The information systems that collectively provide name/address resolution service for SBIWTP are fault-tolerant and implement internal/external role separation.

4.4.17 (SC-23) Session Authenticity

Control: The information system protects the authenticity of communications sessions

Status: This control is currently associated with POA&M #8

Implementation:

System Specific Control

The System protects the authenticity of communications sessions.

4.4.18 (SC-28) Protection of Information at Rest

Control: The information system protects the confidentiality and integrity of information at rest.

Implementation:

System Specific Control

The System protects the confidentiality and integrity of all of the System data related to the SBIWTP SCADA operations that is at rest or stored in the backup servers.

4.5 (PM) Program Management

4.5.1 (PM-1) Program Management Policy and Procedures

Control: The organization:

- a. Develops and disseminates an organization-wide information security program plan that:
 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b.
- b. Reviews the organization-wide information security program plan annually;
- c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
- d. Protects the information security program plan from unauthorized disclosure and modification.

Implementation:

System Specific Control

SBIWTP has taken the following actions to implement organization-wide information security program:

- a. Developed and disseminated an organization-wide information security program plan that:
 - a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
 - b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among SBIWTP officials, and proper compliance;
 - c. Reflects coordination among organizational entities responsible for the different aspects of information security ranging from technical, physical, personnel, cyber-physical; and
 - d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
- b. Reviews the organization-wide information security program plan during information system authorization, reauthorization, and at instances of significant change to the information system;
- c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
- d. Protects the information security program plan from unauthorized disclosure and modification.

4.5.2 (PM-2) Senior Information Security Officer

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Implementation:

System Specific Control

The SBIWTP has appointed a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain the organization-wide information security program.

4.5.3 (PM-3) Information Security Resources

Control: The organization:

- a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
- b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
- c. Ensures that information security resources are available for expenditure as planned

Implementation:

System Specific Control

SBIWTP has taken the following actions to manage resources for the organization-wide information security program:

- a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
- b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
- c. Ensures that information security resources are available for expenditure as planned

4.5.4 (PM-4) Plan of Action and Milestones

Control: The organization:

- a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
 1. Are developed and maintained;
 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 3. Are reported in accordance with OMB FISMA reporting requirements.
- b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Implementation:

System Specific Control

SBIWTP has taken the following actions to manage plans of action and milestones for the organization-wide information security program:

- a. Implemented a process for ensuring that plans of action and milestones for the security program and associated SBIWTP information systems:
 - a. Are developed and maintained;
 - b. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 - c. Are reported in accordance with OMB FISMA reporting requirements.
- b. Reviews plans of action and milestones for consistency with the SBIWTP risk management strategy and enterprise-wide priorities for risk response actions.

4.5.5 (PM-5) Information System Inventory

Control: The organization develops and maintains an inventory of its information systems.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP has developed and continually maintains an inventory of its information systems.

4.5.6 (PM-6) Information Security Measures of Performance

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP develops, monitors, and reports on the results of information security measures of performance.

4.5.7 (PM-7) Enterprise Architecture

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP develops an enterprise architecture with consideration for information security and the resulting risk to SBIWTP operations, organizational assets, individuals, other organizations, and the Nation.

4.5.8 (PM-8) Critical Infrastructure Plan

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

4.5.9 (PM-9) Risk Management Strategy

Control: The organization:

- a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
- b. Implements the risk management strategy consistently across the organization; and
- c. Reviews and updates the risk management strategy annually or as required, to address organizational changes

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP:

- a. Develops a comprehensive strategy to manage risk to SBIWTP operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
- b. Implements the risk management strategy consistently across the all of the SBIWTP; and
- c. Reviews and updates the risk management strategy annually or as required, to address organizational changes

4.5.10 (PM-10) Security Authorization Process

Control: The organization:

- a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
- b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
- c. Fully integrates the security authorization processes into an organization-wide risk management program.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP:

- a. Manages (i.e., documents, tracks, and reports) the security state of SBIWTP information systems and the environments in which those systems operate through security authorization processes;
- b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
- c. Fully integrates the security authorization processes into an organization-wide risk management program.

4.5.11 (PM-11) Mission/Business Process Definition

Control: The organization:

- a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
- b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary until achievable protection needs are obtained. ‘

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP:

- a. Defines mission/business processes with consideration for information security and the resulting risk to SBIWTP operations, organizational assets, individuals, other organizations, and the Nation; and
- b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary until achievable protection needs are obtained.

4.5.12 (PM-12) Insider Threat Program

Control: The organization implements an insider threat program that includes a cross-discipline insider threat Incident Handling Team .

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP implements an insider threat program that includes a cross-discipline insider threat Incident Handling Team.

4.5.13 (PM-13) Information Security Workforce

Control: The organization establishes an information security workforce development and improvement program.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP establishes an information security workforce development and improvement program.

4.5.14 (PM-14) Testing, Training, and Monitoring

Control: The organization:

- a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
 - 1. Are developed and maintained; and
 - 2. Continue to be executed in a timely manner;
- b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP:

- a. Implements a process for ensuring that SBIWTP plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
 - a. Are developed and maintained; and
 - b. Continue to be executed in a timely manner;
- b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

4.5.15 (PM-15) Contacts With Security Groups and Organizations

Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

- a. To facilitate ongoing security education and training for organizational personnel;
- b. To maintain currency with recommended security practices, techniques, and technologies; and
- c. To share current security-related information including threats, vulnerabilities, and incidents.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP establishes and institutionalizes contact with selected groups and associations within the security community:

- a. To facilitate ongoing security education and training for organizational personnel;
- b. To maintain currency with recommended security practices, techniques, and technologies; and
- c. To share current security-related information including threats, vulnerabilities, and incidents.

4.5.16 (PM-16) Threat Awareness Program

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Implementation:

System Specific Control

Through the organization-wide information security program, SBIWTP implements a threat awareness program that includes a cross-organization information-sharing capability.

APPENDIX A SYSTEM STEWARD AND AO RESPONSIBILITIES

Business Steward³:

A Business Steward is a management official to whom responsibility for an agency mission objective is assigned, typically a Branch Chief or Division Director, and who directs or controls the budget, personnel, and information resources to accomplish that mission. The Business Steward is responsible for the following activities under his or her area of responsibility:

- Determining the level of data or information sensitivity;
- Determining the level of system criticality;
- Assessing risk to, and vulnerabilities of, agency information resources periodically, and responding in a coordinated agency-wide manner to resolve vulnerabilities and address risk either by control measures or by acknowledging it as a "residual risk;"
- Establishing and maintaining an SSP, contingency plan, disaster recovery plan, and continuity of operations plan (COOP) and personally accrediting and authorizing the plans and the establishment, operation, change, and retirement of the resource;
- Assigning the technical steward(s) for the information resource;
- Determining the access rights/restrictions for system users;
- Conducting risk and vulnerability assessments periodically, including tests of security and contingency plans.
- Establishing and enforcing procedures needed to create an appropriate trust environment, when work must proceed before required background checks are available (unclassified environment only).

Technical Steward:

A Technical Steward is someone, other than the Business Steward, who performs as either a principal investigator or principal user of an information system or as the principal information technology professional responsible for the system, ensuring that the specified functional characteristics of the system are produced as authorized by the Business Steward. The Technical Steward is responsible for ensuring that systems and applications function in compliance with all appropriate IRM laws, policies, and standards and in accordance with her or his organization's protocols and procedures, as established in the applicable system security plan (SSP). This responsibility includes:

- Planning, designing, testing, implementing, and operating systems and technologies – whether new or updated, carefully and in collaboration with peers and agency-level technical staff, to ensure the overall security and integrity of SBIWTP information resources;
- Managing security requirements;
- Applying access restrictions directed by the Business Steward;
- Taking necessary corrective actions immediately when a critical or sensitive system or information resource is discovered to have a serious vulnerability.
- Identifying and taking necessary corrective actions to reduce risks, nonstandard conditions, and unauthorized activities;
- Maintaining inventories of information resource assets, e.g., hardware, software, and data and providing those to agency officials as needed;

³ <http://intraspn.cdc.gov/maso/policy/Doc/policy300.htm>

- Determining, according to the established standard, when an individual is required to sign a Confidentiality Agreement, assuring that the Agreement reflects currently assigned accesses and authorities and that it is signed and on file before the individual is provided with the intended accesses.

Security Steward:

A Security Steward is someone, other than the Business Steward and normally not a Technical Steward, who is formally designated as the ombudsman for information protection and systems security (IPASS) for the system. Each general support system and each major application shall have a designated Security Steward.

The Security Steward is responsible for:

- Advising both the Business and Technical Stewards on IPASS matters throughout the development life-cycle.
- Advising the Technical Steward on the evaluation of requests for exceptions to standard procedures and conditions.
- Evaluating the completeness and appropriateness of IPASS control measures, and collaborating with appropriate parties on the security, COOP, training and other plans.
- Monitoring operations informally and assuring that both electronic logs are kept and reviewed and formal audits are conducted periodically.

Authorizing Official (AO)

The AO has been "...assigned to the respective heads of the SBIWTP organizations that are financially and programmatically responsible for their respective information systems. This authority shall reside at a level no lower than Division Director or equivalent."⁴

As the senior management official or executive with the authority to approve the operation of the information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, the AO assumes responsibility and is accountable for the risks of operating the system. The AO's decision to authorize operation should rely primarily on the compiled system security plan (SSP), the Risk Mitigation Worksheets (RMW), and the Plan of Action and Milestones (POA&M) for reducing or eliminating information system vulnerabilities. In making the security accreditation decision to authorize operations of the system, the AO explicitly accepts the residual risk to SBIWTP operations or SBIWTP assets.

⁴ J. D. Seligman memorandum dated 03/19/2003, *Designated Approving Authority for CDC Information Systems Security*.