I. PROCEDURE SUMMARY

- This procedure provides the Site with written guidance to maintain compliance with Reliability Standard CIP-003. The Standard requires the identification of a CIP Senior Manager, documentation regarding the delegation of CIP authority, periodic review and approval of Cyber Security Policies, implementation of documented Cyber Security Plans, and declaring and responding to CIP Exceptional Circumstances.

- Applicability: GO, GOP

    - The Site's Low Impact BES Cyber Systems are subject to the requirements of this procedure.

    - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are exempt from the requirements of this procedure.

- **The effective date of this procedure revision is the Asset Management date.

REVISION INDEX

Revision	Section Revised	Comments	Effective Date
rev00	All	Initial Release	

II. TABLE OF CONTENTS

III. DETAILED PROCEDURE

1.0 PURPOSE

The purpose of this procedure is to specify consistent and sustainable security management controls that establish responsibility and accountability to protect Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- For site-specific information (which is italicized and underlined), refer to the Site Data Sheet or CIP Site Data Sheet as applicable. All specific site information needed will have been identified in previous sections.

2.0 REFERENCES

2.1 Reliability Standard CIP-002-5.1a, “Cyber Security – BES Cyber System Categorization”

2.2 NERC Standard CIP-003-8, “Cyber Security – Security Management Controls”

2.3 SAV-PRO-EOP-004, “Event Reporting”

2.4 Department of Homeland Security Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, October 2009

2.5 NERC Security Guideline for the Electricity Sector: Threat and Incident Reporting, April 1, 2008.

2.6 U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response Form DOE-417, “Electric Emergency Incident and Disturbance Report”

2.7 U.S. Department of Energy DOE-417 instructions

2.8 *PJM Manual 13, “Emergency Operations”*

2.9 *ISO New England Operating Procedure No. 10, “Emergency Incident and Disturbance Notifications”*

2.10 *New York Independent System Operator Manual 15, “Emergency Operations Manual”*

2.11 *ERCOT Nodal Operating Guides Section 3: ERCOT and Market Participant Responsibilities; Sections 3.2.3, 3.8*

3.0 DEFINITIONS

Capitalized terms used herein and not defined herein shall have the meanings as described to such terms in the NERC “Glossary of Terms used in NERC Reliability Standards” located at http://www.nerc.com.

3.1 **“Application Whitelisting”** – The practice of authorizing only the approved software applications and processes that are permitted to be present and active on a computer system.

3.2 **"BES Cyber Asset (BCA)"** – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

3.3 **"BES Cyber System (BCS)"** – One or more BES Cyber Asset logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

3.4 **"Bulk Electric System (BES)"** – See NERC "Glossary of Terms Used in NERC Reliability Standards" definition.

3.5 **"CIP Senior Manager"** – A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

3.6 **"CIP Exceptional Circumstance"** – A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

3.7 **"Cyber Assets"** – Programmable electronic devices, including the hardware, software, and data in those devices.

3.8 **"Cyber Security Incident"** – A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Note: Cyber Security Incidents may be identified by methods such as:

- Direct observation – observing intrusion through a security perimeter, finding damage to BES Cyber Systems, observing abnormal system or component behavior, etc.
- Automated detection – network monitors, antivirus or malware monitors, intrusion alarms, Cyber System component failure alarms, etc.

3.9 **"Dial-Up Connectivity"** – A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

3.10 **"Electronic Access Control or Monitoring Systems (EACMS)"** – Cyber Assets that perform electronic access control or electronic access monitoring of

the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

3.11 **"Electronic Access Point (EAP)"** – A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

3.12 **"Electronic Security Perimeter (ESP)"** – The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

3.13 **"Element"** – Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An Element may be comprised of one or more components.

3.14 **"Emergency or BES Emergency"** – Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.

3.15 **"Executable Only"** – Software, applications, etc. that are only allowed to be run as an executable file and do not allow for modifications or updates that alter the original programming or base code.

3.16 ***"*****External Routable Connectivity (ERC)*****"*** – The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

3.17 **"Facility"** – A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)

3.18 **"Interactive Remote Access"** – User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

3.19 **"Intermediate System"** – A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

3.20 **"Live Operating System"** – An operating system that loads from a removable storage device (CD/DVD, external data drive, USB drive) as opposed to from internal storage devices in a computer.

3.21 **"Malicious Code"** – Any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system.

3.22 "Multi-Factor Authentication" – Use of more than one (1) authenticator, which may include, but is not limited to:

- Something the individual seeking access knows, such as passwords or PINs. (This does not include User ID.)
- Something the individual seeking access has, such as tokens, digital certificates, or smart cards.
- Something the individual seeking access is, such as fingerprints, iris scans, or other biometric characteristics.

3.23 "Physical Access Control Systems (PACS)" – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

3.24 "Physical Security Perimeter (PSP)" – The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

3.25 "Protected Cyber Assets (PCAs)" – One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

3.26 "Read-Only" – A read-only file or storage device contains data that cannot be modified or deleted. While data can be accessed or "read" from a read-only file or device, new data cannot be added or "written" to the device.

3.27 "Reliable Operation" – Operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

3.28 "Removable Media (RM)" – Storage media that:

(1) are not Cyber Assets,

(2) are capable of transferring executable code,

(3) can be used to store, copy, move, or access data, and

(4) are directly connected for 30 consecutive calendar days or less to a:

- BES Cyber Asset,
- network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
- Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

3.29 "Reportable Cyber Security Incident" – A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

3.30 "System Hardening" – In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. Examples include: elimination of unnecessary accounts and privileges, elimination of unused software and features, security patch updating, disabling ports, antivirus installation, disabling cookies, encryption, logical access controls, default setting adjustment, etc.

3.31 "Transient Cyber Asset (TCA)" – A Cyber Asset that is:

(1) capable of transmitting or transferring executable code,

(2) not included in a BES Cyber System,

(3) not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and

(4) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:

- BES Cyber Asset,
- network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
- PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

4.0 RESPONSIBILITIES

4.1 The Corporate Senior Management shall designate the *CIP Senior Manager*.

4.2 *CIP Senior Manager* shall:

4.2.1 Maintain accurate and up-to-date documentation of the *CIP Senior Manager* and CIP Authority Delegate(s).

4.2.2 Ensure that all documented cyber security plans are effectively implemented:

4.2.2.1 The Site personnel are trained on the site's cyber security program and practices.

4.2.2.2 Appropriate methods are used to control physical access to The Site's BES Cyber Assets, BES Cyber Systems, and their associated Physical Security Perimeters.

4.2.2.3 Electronic Security Perimeters and Electronic Access Points are defined and protected.

4.2.2.4 Electronic Access Control processes for *External Routable Connectivity, Interactive Remote Access* sessions, and Dial-up Connectivity are implemented.

4.2.2.5 A Cyber Security Incident Response Exercise is performed in a timely manner and that the Cyber Security Incident Plan is updated as necessary.

4.2.2.6 Screening of Transient Cyber Assets and Removable Media occurs prior to connecting to The Site's BES Cyber Systems.

4.2.3 Review and approve this cyber security program document in accordance with the defined periodicity requirements.

4.2.4 Coordinate with the Asset Manager and Operations Supervisor on Cyber Security Incident investigation, classification, reporting, response, recovery, and mitigation.

4.2.5 Declare and terminate CIP Exceptional Circumstances.

4.2.6 Invoke or oversee alternate processes in the event of a CIP Exceptional Circumstance.

4.3 CIP Authority Delegate(s) shall ensure that applicable delegated actions and responsibilities are carried out.

4.4 Asset Manager shall coordinate with the *CIP Senior Manager* or delegate and Operations Supervisor on Cyber Security Incident investigation, classification, reporting, response, recovery, and mitigation.

4.5 Operations Supervisor shall:

4.5.1 Take appropriate actions to respond to Cyber Security Incidents.

4.5.2 Notify the Asset Manager and *CIP Senior Manager* or delegate of all Cyber Security Incidents.

4.5.3 Coordinate with the Asset Manager and *CIP Senior Manager* or delegate on Cyber Security Incident investigation, classification, reporting, response, recovery, and mitigation.

4.6 Security personnel (if any) shall assist in the investigation, classification, reporting, response, recovery, and mitigation of Cyber Security Incidents as requested.

4.7 Technical personnel shall assist in the investigation, classification, reporting, response, recovery, and mitigation of Cyber Security Incidents as requested.

4.8 The Site personnel are responsible for:

4.8.1 Performing tasks in accordance with the policies and processes outlined in this CIP program.

4.8.2 Notification to appropriate management of any actual or suspected violation of the Site's Physical Security Control Plan.

4.8.3 Notification to the Operations Supervisor of any actual or suspected Cyber Security Incidents.

4.8.4 Maintenance and implementation of primary physical controls such as: physical boundaries, keyed access, and badge readers. Additional physical access control mechanisms may be utilized to bolster The Site's defense-in-depth strategy.

4.8.5 Ensuring the threat of Malicious Code is mitigated prior to connection to the Site's BES Cyber System via On-Demand Device Acceptance or Advance Programmatic Acceptance and that the appropriate evidence is documented.

5.0 DETAILS

5.1 The Site's *CIP Senior Manager* or delegate shall ensure that the Site's maintains the following cyber security program appendices. Policies and processes pertaining to *Low Impact BES Cyber Systems* shall be addressed within these program appendices as required by NERC Standard CIP-003 (Ref. Attachment 1, "Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems") at a minimum.

5.1.1 Appendix A, "Cyber Security Awareness"

5.1.2 Appendix B, "Physical Security Controls"

5.1.3 Appendix C, "Electronic Access Controls"

5.1.4 Appendix D, "Cyber Security Incident Response"

5.1.5 Appendix E, "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation"

5.2 The Site's *CIP Senior Manager* shall approve the cyber security program annually, not to exceed fifteen (15) calendar months. See Attachment 4, "CIP Program Annual Review Form."

5.3 The Fleet Senior Management shall assign a *CIP Senior Manager* with overall authority and responsibility for leading and managing the implementation of, and adherence to, the requirements within the applicable NERC CIP Standards using Attachment 2, "*CIP Senior Manager* Designation Form" or equivalent.

5.3.1 Designation of the *CIP Senior Manager* shall include:

5.3.1.1 Name and title of the *CIP Senior Manager*

5.3.1.2 Date of designation

5.3.1.3 Signed approval from Fleet Senior Management

5.3.2 Changes to the *CIP Senior Manager* shall be documented within thirty (30) calendar days of the change.

5.3.3 The *CIP Senior Manager* may delegate authority for specific actions to a delegate or multiple delegates (where allowed by the CIP Standards) using Attachment 3, "CIP Authority Delegation Form" or equivalent. Delegations shall include:

5.3.3.1 Name or title of the delegate

5.3.3.2 Specific actions delegated

5.3.3.3 Date of delegation

5.3.3.4 Signed approval from the *CIP Senior Manager*

5.3.4 Changes to the CIP Authority Delegation shall be updated within thirty (30) calendar days of the change.

5.4 If the Site is experiencing an imminent or active emergency, the Site's personnel shall determine if the classification of the Incident meets the definition of a CIP Exceptional Circumstance (Ref. Section 3.0, "Definitions" and Attachment 5, "CIP Exceptional Circumstance Flowchart"). If so:

5.4.1 The incident shall be declared a CIP Exceptional Circumstance for which the date and time shall be logged.

5.4.1.1 Status notifications of emergency operations and the declared CIP Exceptional Circumstance shall be made to Senior Management and site personnel as feasible.

5.4.1.2 The *CIP Senior Manager* or delegate shall invoke or oversee the alternate processes being used to address the CIP Exceptional Circumstance.

> Note: The Site's personnel are authorized to take actions as are necessary where any delay may jeopardize safety or BES reliability. These actions may be in exception to previously defined CIP-related procedures or regulations.

5.4.2 Upon completion of any and all necessary emergency actions, the CIP Exceptional Circumstance shall be terminated with the date and time logged. Compliance exceptions are not authorized after this point.

5.4.2.1 Termination of the CIP Exceptional Circumstance shall be communicated to Senior Management and site personnel.

5.4.2.2 Assessments shall be made to determine how to restore security, reliability, and normal operation as necessary.

5.4.2.3 The Site's personnel shall document the CIP Exceptional Circumstance (cause, timeframes, actions taken, recovery actions, etc.).

6.0 RECORDS

6.1 The Site shall ensure appropriate reports, data sheets, spreadsheets, specifications, emails, letters, procedures, logs, compliance records, memoranda, or other dated documentation are retained as evidence of compliance for a minimum period equal to the longest of the following:

- Three (3) calendar years;
- The full time period since the end of the last audited period;
- For specific evidence that is related to a compliance violation, the period until mitigation is complete and approved by the Compliance Enforcement Authority; or
- For specific evidence that is part of any other investigation, the period specified by the Compliance Enforcement Authority.

6.2 The Site shall keep the last audit records, and all requested and submitted subsequent audit records.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

7.1 (CIP-003-8 R1) Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

7.1.1 (1.2) For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

(1.2.1) Cyber security awareness;

(1.2.2) Physical security controls;

(1.2.3) Electronic access controls;

(1.2.4) Cyber Security Incident response;

(1.2.5) Transient Cyber Assets and Removable Media malicious code risk mitigation; and

(1.2.6) Declaring and responding to CIP Exceptional Circumstances.

7.2 (CIP-003-8 R2) Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

7.3 (CIP-003-8 R3) Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

7.4 (CIP-003-8 R4) The Responsible Entity shall implement a documented process to delegate authority unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

8.0 KEY WORDS

8.1 BES Cyber Asset

8.2 BES Cyber System

8.3 CIP Exceptional Circumstance

8.4 CIP Program

8.5 CIP Senior Manager

8.6 Cyber Assets

8.7 Cyber Security

8.8 Cyber Security Awareness

8.9 Cyber Security Program

8.10 Delegate

8.11 Electronic Access

8.12 Electronic Security Perimeter

8.13 Incident Response

8.14 Physical Security Perimeter

8.15 Removable Media

8.16 Security Policy

8.17 Transient Cyber Asset

9.0 ATTACHMENTS

9.1 Attachment 1: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

9.2 Attachment 2: CIP Senior Manager Designation Form

9.3 Attachment 3: CIP Authority Delegation Form

9.4 Attachment 4: CIP Program Annual Review Form

9.5 Attachment 5: CIP Exceptional Circumstance Flowchart

9.6 Appendix A: Cyber Security Awareness

Refer to Appendix A for associated attachments.

9.7 Appendix B: Physical Security Controls

Refer to Appendix B for associated attachments.

9.8 Appendix C: Electronic Access Controls

Refer to Appendix C for associated attachments.

9.9 Appendix D: Cyber Security Incident Response

Refer to Appendix D for associated attachments.

9.10 Appendix E: Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

Refer to Appendix E for associated attachments.

ATTACHMENT 1 **Page 1 of 3**
Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

---

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their *high* or *medium impact BES Cyber System*s to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the *low impact BES Cyber Systems* within the asset, and (2) the *Cyber* Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing *low impact BES Cyber System(s)* identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a *low impact BES Cyber System(s)* and a Cyber Asset(s) outside the asset containing *low impact BES Cyber System(s)*;

ii. using a routable protocol when entering or leaving the asset containing the *low impact BES Cyber System(s)*; and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to *low impact BES Cyber System(s)*, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

ATTACHMENT 1 **Page 2 of 3**
Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to *low impact BES Cyber Systems* through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a *low impact BES Cyber System* (per Transient Cyber Asset capability):

- Review of antivirus update level.

- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a *low impact BES Cyber System*.

ATTACHMENT 2 **Page 1 of 1**
CIP Senior Manager **Designation Form**

CIP SENIOR MANAGER **DESIGNATION**

The following individual has been designated as the *Critical Infrastructure Protection (CIP) Senior Manager* with overall authority and responsibility for leading and managing implementation of, and continuing adherence to, the applicable requirements within the NERC CIP Standards.

CIP Senior Manager	
Name	
Title	
Effective Date of Designation	

This approved designation supersedes all previous *CIP Senior Manager* designations and releases the previous *CIP Senior Manager* from all related duties on the Effective Date of Designation above.

Approver (Senior Management)	
Name	
Title	
Organization	
Signature & Approval Date	

ATTACHMENT 3 **Page 1 of 1**
CIP Senior Manager Delegation Form

CIP AUTHORITY DELEGATION

The following individual has been delegated and assigned with Critical Infrastructure Protection (CIP) authority by the ***CIP Senior Manager*** for the specific actions identified below.

CIP Authority Delegate	
Name (optional)	
Title	
Effective Date	

Actions Delegated (check all that apply)

- ☐ Proxy signatory for ***CIP Senior Manager*** where allowed by the CIP Standards. Note: Approval of cyber security policies cannot be delegated.
- ☐ Preparation, general updating, and/or review of cyber security policy documents.
- ☐ Preparation, general updating, and/or review of CIP-related supporting evidence documents (e.g., CIP-002 Impact Evaluation, Cyber Asset Lists).
- ☐ Additional management to the adherence of CIP Standards and related documents at the facility.
- ☐ Distribution of Cyber Security Awareness material.
- ☐ Enforcement of Physical Security protocols.
- ☐ Enforcement of Electronic Security of BES Cyber Systems.
- ☐ Cyber Security Incident Response support.
- ☐ Enforcement of Transient Cyber Asset and Removable Media risk mitigation protocols.
- ☐ Declaration of CIP Exceptional Circumstances.
- ☐ Other. (Attach additional description page(s). Each additional page must be initialed & dated by ***CIP Senior Manager***.)

CIP Senior Manager **Approval**	
Name	
Signature & Date	

This delegation of authority remains in effect until formally withdrawn as indicated below.

CIP Senior Manager **Withdrawal** (not required to be the same as the approving ***CIP Senior Manager***)	
Name	
Signature & Date	

ATTACHMENT 4 **Page 1 of 1**
CIP Program Annual Review Form

CIP PROGRAM ANNUAL REVIEW

The following documents shall be approved by the ***CIP Senior Manager*** annually, not to exceed fifteen (15) calendar months, in accordance with the Requirements of NERC Standards CIP-002 and CIP-003. This action cannot be delegated.

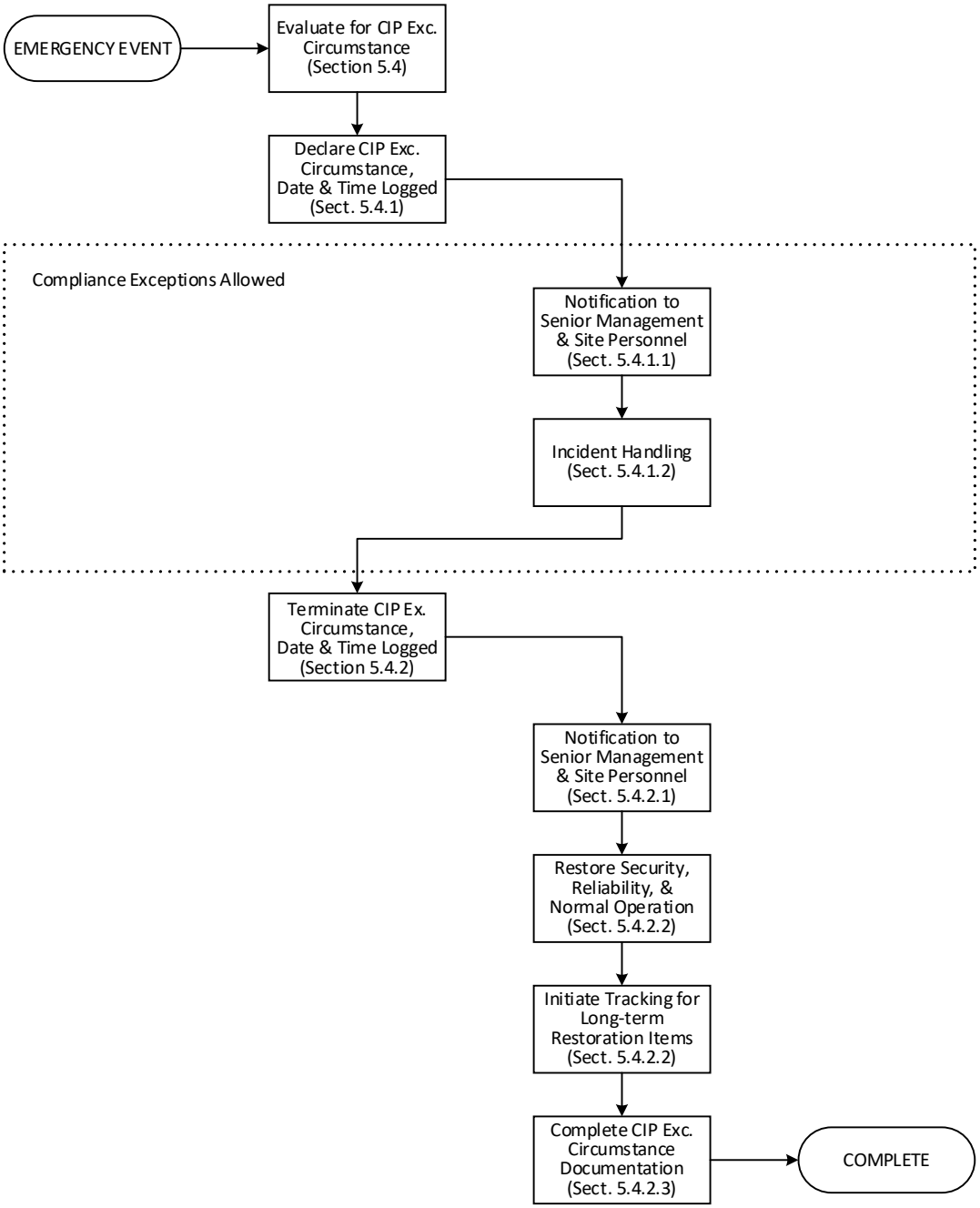
#	Document	Activity	Date	Reviewer's Initials
1	Impact Evaluation***	Verify Impact Rating has not changed per current CIP Standards. Take action as necessary.		
2	Cyber Asset Inventory	Ensure all Cyber Assets are identified and classified accurately.		
3	Network Diagram	Ensure ESPs, Electronic Access Points, Electronic Access Control or Monitoring System, etc. are secure and clearly diagrammed.		
4	CIP-002 Procedure (Ref. SAV-PRO-CIP-002)	Ensure procedure is aligned with current NERC Standard CIP-002.		
5	CIP-003 Procedure (Ref. SAV -PRO-CIP-003)	Ensure procedure is aligned with current NERC Standard CIP-003.		
6	Cyber Security Awareness Plan*** (Ref. SAV -PRO-CIP-003 Appendix A)	Ensure plan is aligned with current NERC Standard CIP-003 and effectively implemented.		
7	Physical Security Controls Plan*** (Ref. SAV -PRO-CIP-003 Appendix B)	Ensure plan is aligned with current NERC Standard CIP-003 and effectively implemented.		
8	Electronic Access Controls Plan*** (Ref. SAV -PRO-CIP-003 Appendix C)	Ensure plan is aligned with current NERC Standard CIP-003 and effectively implemented.		
9	Cyber Security Incident Response Plan*** (Ref. SAV -PRO-CIP-003 Appendix D)	Ensure plan is aligned with current NERC Standard CIP-003 and effectively implemented.		
10	Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation Plan*** (Ref. SAV -PRO-CIP-003 Appendix E)	Ensure plan is aligned with current NERC Standard CIP-003 and effectively implemented.		

*** Review of this document is mandatory per the NERC CIP Standards.

The above cyber security documents have been reviewed and are approved for use.

CIP Senior Manager	
Name	
Signature & Approval Date	

ATTACHMENT 5
CIP Exceptional Circumstance Flowchart



APPENDIX A

Cyber Security Awareness
Page 1 of 2

1.0 PURPOSE

This appendix to procedure SAV-PRO-CIP-003 provides written guidance on how to establish and reinforce Cyber Security Awareness with Site personnel in compliance with NERC Standard CIP-003.

This appendix serves as the Site's Cyber Security Awareness Plan.

2.0 REFERENCES

Refer to the main body of this procedure for reference documents.

Where section numbers are referenced within this appendix, the section is local to this appendix unless otherwise specified.

3.0 DEFINITIONS

Refer to the main body of this procedure.

4.0 RESPONSIBILITIES

Refer to the main body of this procedure.

5.0 DETAILS

5.1 The *CIP Senior Manager* or delegate shall ensure that appropriate personnel and contractors (per their assigned job function or task) are trained on Site's cyber security program and subsequent electronic and/or physical security practices.

5.1.1 This may be accomplished using one or more of the following methods:

5.1.1.1 Formal training session/class

5.1.1.2 "Read and sign" distribution

5.1.1.3 Onsite arrival orientation

5.1.1.4 Pre-job brief

5.1.2 The Site shall retain documented evidence of the execution of the Site's cyber security program training activities. When possible, training material should be included as evidence.

5.2 The Site shall provide ongoing Cyber Security Awareness information that reinforces cyber security practices.

5.2.1 This may be accomplished using one or more of the following methods:

5.2.1.1 Emails or memos

APPENDIX A

Cyber Security Awareness
Page 2 of 2

5.2.1.2 Presentations or meetings

5.2.1.3 Posters or brochures

5.2.1.4 Company website, intranet, or newsletter

5.2.2 The Site shall retain documented evidence of the execution of Site's cyber security awareness activities for compliance purposes. When possible, the awareness material should be included as evidence.

5.2.3 All personnel with authorized electronic or authorized unescorted physical access to Site's BES Cyber Systems shall be provided Cyber Security Awareness information at least once every fifteen (15) calendar months.

6.0 RECORDS

Refer to the main body of this procedure.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

This appendix is written in accordance with CIP-003-8 Attachment 1 Section 1. Refer to the main body of this procedure and Attachment 1, "Required Sections for Cyber Security Plan(s) for Assets Containing *Low Impact BES Cyber Systems*" for specific requirements.

8.0 KEY WORDS

Refer to the main body of this procedure.

9.0 ATTACHMENTS

None

APPENDIX B

Physical Security Controls
Page 1 of 6

1.0 PURPOSE

This appendix to procedure SAV-PRO-CIP-003 provides written guidance on how to establish and reinforce Physical Security Controls for Site's facilities and personnel in compliance with NERC Standard CIP-003.

This appendix serves as Site's Physical Security Controls Plan.

2.0 REFERENCES

Refer to the main body of this procedure for reference documents.

Where section numbers are referenced within this appendix, the section is local to this appendix unless otherwise specified.

3.0 DEFINITIONS

Refer to the main body of this procedure.

4.0 RESPONSIBILITIES

Refer to the main body of this procedure.

5.0 DETAILS

5.1 Site personnel shall notify appropriate management of any violation or suspected violation of the Site's Physical Security Control Plan. (Ref. Appendix D, "Cyber Security Incident Response")

5.2 Access Authorization

5.2.1 The Site's Physical Security Plan logically layers Physical Security Perimeters (PSPs) with Authorization Levels (ALs). The following ALs are recognized at the Site:

5.2.1.1 Access through the facility PSP (including secured buildings/areas that do not require higher ALs) is granted by the Asset Manager via the GENERAL SITE ACCESS AL.

5.2.1.2 Access through PSPs containing BES Cyber System (BCS) devices or their associated Electronic Access Control or Monitoring Systems (EACMS) is granted by the *CIP Senior Manager* or delegate via the BCS AUTHORIZED AL.

5.2.2 The Site shall maintain documentation of all personnel's Authorization Levels similar to Attachment B1, "Physical Security Authorization Log". If the site uses a different list (not Attachment B1) to track personnel access

APPENDIX B

Physical Security Controls
Page 2 of 6

levels or perimeter authorizations, the content should be similar what is outlined in Attachment B1.

5.2.3 Employee Access

5.2.3.1 Personnel who are granted GENERAL SITE ACCESS are pre-authorized to enter the facility PSP but are restricted from entering any BCS or EACMS PSP unless they are also granted BCS AUTHORIZED access or are continuously escorted by an authorized individual.

5.2.3.2 Personnel who are BCS AUTHORIZED are pre-authorized to enter any PSP that contains BCS or associated EACMS devices. LOW BCS AUTHORIZED personnel are authorized to serve as visitor escorts for their authorized PSPs.

5.2.4 Contractor Access

5.2.4.1 Contractors are restricted from entering any PSPs until access has been granted for the time of the visit.

5.2.4.2 Contractors, upon initial arrival, will check in with the appropriate site personnel and sign-in. Contractors who require physical access to the facility for a duration exceeding one (1) day may be granted GENERAL SITE ACCESS for subsequent visits, which will not require manual sign-in each time they report to the facility.

5.2.4.3 Contractors will review instructions on physical access requirements and any other requirements under the Site's cyber security program related to their task.

5.2.4.4 Contractors without authorization are restricted from entering any BCS or EACMS PSPs unless continuously escorted by an authorized individual. Contractors who require physical access to a BCS or EACMS PSP for a duration exceeding one (1) day may be granted BCS AUTHORIZED access, which will not require continuous escort.

5.2.5 Visitor Access

5.2.5.1 Visitors are restricted from entering any PSPs until access has been granted for the time of the visit.

5.2.5.2 Visitors, upon arrival, will check in with the appropriate site personnel and sign-in.

5.2.5.3 Visitors will review instructions on physical access requirements.

APPENDIX B

Physical Security Controls
Page 3 of 6

5.2.5.4 Visitors are restricted from entering any BCS or EACMS PSPs unless continuously escorted by an authorized individual.

5.3 Physical Security Controls

The Site maintains the following physical security controls as identified in the CIP Site Data Sheet. These controls apply to the facility PSP and other PSPs, within the facility PSP, that are specific to locations where BCS and EACMS devices are housed—see the referenced sections for details.

Control	General Description
Perimeter Fencing (Section 5.3.1)	See the CIP Site Data Sheet
Main Security Gate (Section 5.3.2)	See the CIP Site Data Sheet
Ancillary Gates (Section 5.3.3)	See the CIP Site Data Sheet
Sign-in Log (Section 5.3.4)	Contractors & Visitors, upon arrival at the facility, will sign in prior to gaining access to other areas within the facility.
Security Cameras (Section 5.3.5)	See the CIP Site Data Sheet
Badged Access (Section 5.3.6)	See the CIP Site Data Sheet
Hard Keys (Section 5.3.7)	See the CIP Site Data Sheet

5.3.1 *Perimeter Fencing (if applicable, see CIP Site Data Sheet)*

5.3.1.1 The perimeter fence establishes the facility PSP.

5.3.1.2 All perimeter fencing is inspected as part of the walk down conducted by site personnel on a basis defined in the CIP Site Data Sheet. Site personnel check to make sure that the fence is in good working condition and no damage, tampering, attempted subversion, or unauthorized access has occurred.

5.3.1.3 Any damage, tampering, attempted subversion, or unauthorized access to the perimeter fencing identified during the walk down is to be reported to the control room and/or facility management.

APPENDIX B

Physical Security Controls
Page 4 of 6

5.3.2 *Main Security Gate (if applicable, see CIP Site Data Sheet)*

5.3.2.1 The *Main Security Gate* is the primary physical access point on the facility PSP.

5.3.2.2 All individuals shall be processed through the *Main Security Gate* for initial entry to the facility.

5.3.2.3 Individuals with GENERAL SITE ACCESS shall use their individually assigned badge to gain access to the facility.

5.3.2.4 This gate may be monitored by *security camera* (see Section 5.3.5). Site personnel shall visually verify the general identity of Contractors & Visitors using the *security camera* before access is granted and visually verify the Contractor or Visitor's progress to the sign-in location (see Section 5.3.4).

5.3.3 *Ancillary Gates (if applicable, see CIP Site Data Sheet)*

5.3.3.1 Aside from the *Main Security Gate*, there are *number (#) ancillary gates* along the perimeter fence that provide physical access through the facility PSP.

5.3.3.2 *Ancillary gates* may only be used when needed for specific job functions, and only after the user has reported to the site via the *Main Security Gate* (see Section 5.3.2).

5.3.3.3 All *ancillary gates* are closed and locked when not in use.

5.3.3.4 When in use, ingress/egress through *ancillary gates* is monitored by an individual authorized for GENERAL SITE ACCESS or by security camera (see Section 5.3.3).

5.3.4 Sign-in Log

5.3.4.1 The Sign-in Log will be utilized to document the entry and exit of individuals who are not authorized access via one of the ALs described in Section 5.2.1.

5.3.4.2 The Sign-in Log should include:

A. Date

B. Time of entry

C. Time of exit

D. Contractor or Visitor's name

E. Contractor's company (Visitor may indicate "Visitor")

F. Point of contact responsible for Contractor or Visitor

APPENDIX B

Physical Security Controls
Page 5 of 6

5.3.5 *Security Cameras (if applicable, see CIP Site Data Sheet)*

5.3.5.1 There are *(#)* security cameras installed across the facility to provide increased visibility:

Cam #	Camera Type	Visibility Description
See the CIP Site Data Sheet	*See the CIP Site Data Sheet*	*See the CIP Site Data Sheet*

5.3.5.2 *The live camera feeds are monitored by personnel.*

5.3.6 *Badge Access System (if applicable, see CIP Site Data Sheet)*

5.3.6.1 The following areas are secured via badge readers:

A. *See the CIP Site Data Sheet*

5.3.6.2 Access is granted on a “need to know” basis at the minimum level required to perform assigned duties based on an individual’s job function.

5.3.6.3 The individual to whom the badge is assigned holds the ultimate responsibility for the badge.

5.3.7 *Hard Key Management (if applicable, see CIP Site Data Sheet)*

5.3.7.1 The following areas are secured via hard keys:

A. *See the CIP Site Data Sheet*

5.3.7.2 Distribution of hard keys and the individuals responsible for those keys are managed in an onsite physical access control list.

5.3.7.3 Hard keys are collected upon termination of employment or upon a determination that the employee or contractor no longer needs unescorted access to the facility (e.g., retirement, contract termination, job transfer).

5.3.7.4 The individual to whom the key is assigned holds the ultimate responsibility for the key.

5.3.7.5 Lost keys must be immediately reported to the control room or Operations Supervisor.

APPENDIX B

Physical Security Controls
Page 6 of 6

6.0 RECORDS

Refer to the main body of this procedure.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

This appendix is written in accordance with CIP-003-8 Attachment 1 Section 2. Refer to the main body of this procedure and Attachment 1, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems” for specific requirements.

8.0 KEY WORDS

Refer to the main body of this procedure.

9.0 ATTACHMENTS

9.1 Attachment B1: Physical Security Authorization Log

9.2 Attachment B2: Site Layout

ATTACHMENT B1 **Page 1 of 2**
Physical Security Authorization Log

Log Page __1__ of _____

#	Employee Name	Title	Authorization Level	
			Facility PSP	BCS or EACMS PSPs
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Signing below indicates that this list has been validated and is approved.

Asset Manager	***CIP Senior Manager*** **or Delegate**
Printed Name:	Printed Name:
Signature:	Signature:
Date:	Date:

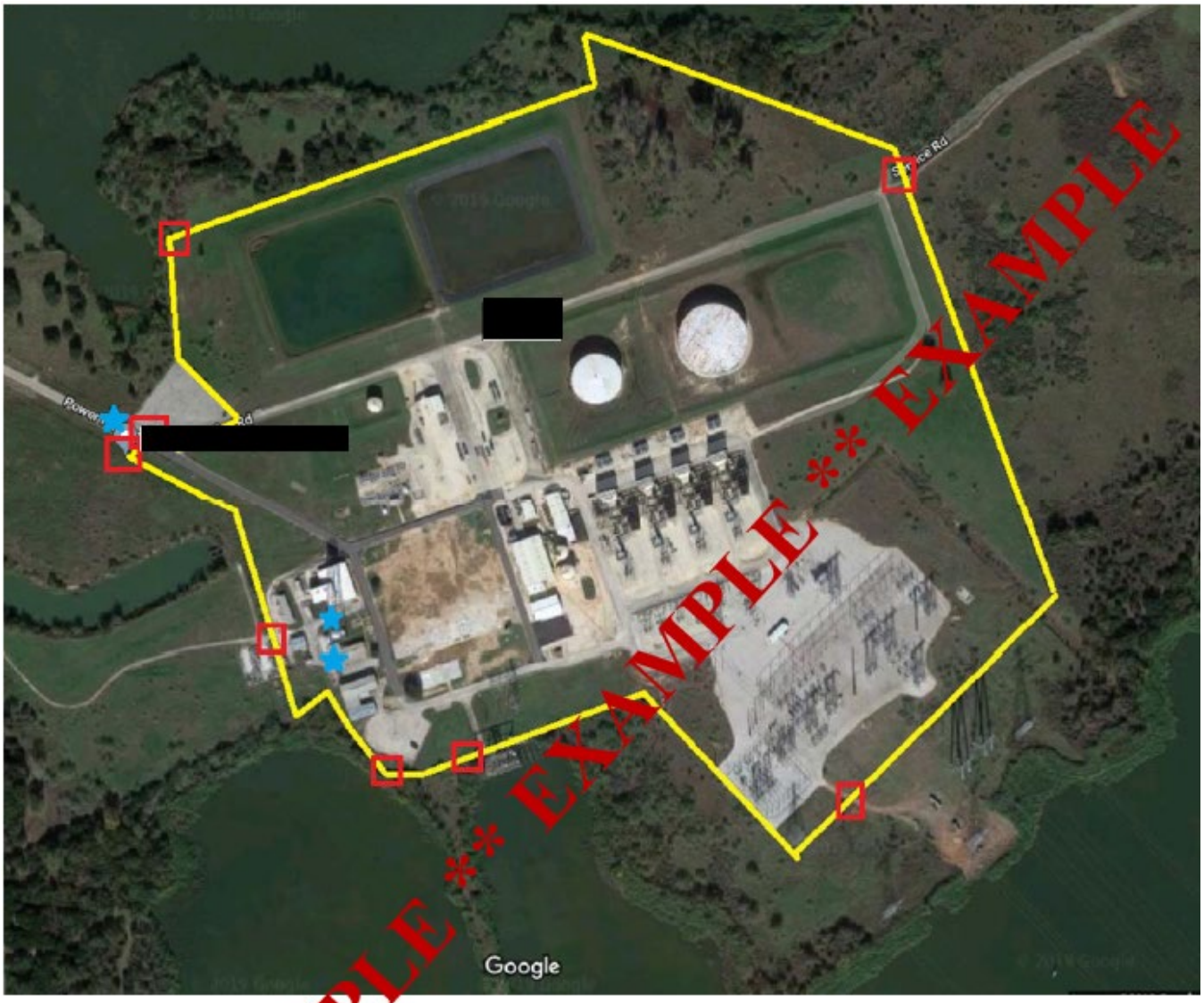
ATTACHMENT B1 **Page 2 of 2**
Physical Security Authorization Log (Continuation Page)

Log Page _____ of _____

#	Employee Name	Title	Authorization Level	
			Facility PSP	BCS or EACMS PSPs

Asset Manager Initials		*CIP Senior Manager* or Delegate Initials	

ATTACHMENT B2
Site Layout



	Perimeter Fencing
	Facility Gates
	Facility Cameras

Note: See CIP Site Data Sheet for actual plant layout.

APPENDIX C

Electronic Access Controls
Page 1 of 3

1.0 PURPOSE

This appendix to procedure SAV-PRO-CIP-003 provides written guidance to ensure that Electronic Access Controls are provided for Cyber Assets within the Site's defined Electronic Security Perimeters in compliance with NERC Standard CIP-003.

This appendix serves as the Site's Electronic Access Controls Plan.

2.0 REFERENCES

Refer to the main body of this procedure for reference documents.

Where section numbers are referenced within this appendix, the section is local to this appendix unless otherwise specified.

3.0 DEFINITIONS

Refer to the main body of this procedure.

4.0 RESPONSIBILITIES

Refer to the main body of this procedure.

5.0 DETAILS

5.1 Inbound and outbound electronic access to an ESP containing one or more BES Cyber Systems is controlled by the following.

Note: The specific implementation of these approved methods is maintained in documents separate from this procedure (Ref. Section 5.2).

5.1.1 *External Routable Connectivity* (if any)

The Electronic Security Perimeter shall be protected via an Electronic Access Control or Monitoring System (EACMS) that does not allow *Interactive Remote Access* to have direct access to BES Cyber Systems. The EACMS shall be configured to:

5.1.1.1 Only allow inbound and outbound access by permissions/rules for communications that are:

- between a BES Cyber System(s) and a Cyber Asset(s) outside the asset containing BES Cyber System(s);
- using a routable protocol when entering or leaving the asset containing the BES Cyber System(s); and

APPENDIX C

Electronic Access Controls
Page 2 of 3

- not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR- 61850-90-5 R-GOOSE).

5.1.1.2 Deny ALL other access by default.

5.1.1.3 For each *Interactive Remote Access* that is deemed necessary (if any), the Site's personnel shall document the business reason for the access permission.

5.1.2 *Interactive Remote Access* Sessions (if any)

Interactive Remote Access sessions shall, where technically feasible:

5.1.2.1 Use encryption between the EACMS and the Cyber Asset initiating communication. If an *Intermediate System* is used, encryption shall be utilized from the EACMS and up to the *Intermediate System* at a minimum.

5.1.2.2 Use Multi-Factor Authentication.

5.1.3 *Dial-up Connectivity* (if any)

Any inbound and outbound connectivity shall be controlled by performing authentication when establishing connectivity, where technically feasible.

5.2 *CIP Senior Manager* or delegate shall ensure that the site's Cyber Asset inventory and diagram documents:

5.2.1 Electronic Security Perimeters (ESPs)

5.2.1.1 All BES Cyber Assets shall be included within a defined ESP.

5.2.2 Electronic Access Points (EAPs), if any

5.2.2.1 All routable connectivity paths to the ESP shall travel through an identified EAP.

5.2.3 *External Routable Connectivity (ERC)*, if any

5.2.4 Electronic Access Control or Monitoring Systems (EACMS), if any

5.2.5 BES Cyber Assets (BCAs)

5.2.6 Protected Cyber Assets (PCAs), if any

5.2.7 Transient Cyber Assets and Removable Media (TCAs and RM)

6.0 RECORDS

Refer to the main body of this procedure.

APPENDIX C

Electronic Access Controls
Page 3 of 3

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

This appendix is written in accordance with CIP-003-8 Attachment 1 Section 3. Refer to the main body of this procedure and Attachment 1, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems” for specific requirements.

8.0 KEY WORDS

Refer to the main body of this procedure.

9.0 ATTACHMENTS

None

APPENDIX D

Cyber Security Incident Response
Page 1 of 9

1.0 PURPOSE

This appendix to procedure SAV-PRO-CIP-003 provides written guidance on how to respond to, classify, report, mitigate, and perform exercises related to Cyber Security Incidents in compliance with NERC Standard CIP-003. This appendix is not intended to illustrate all DOE and NERC reporting thresholds, but does address those related to Cyber Security Incidents, which may include physical intrusions and threats.

This appendix serves as the Site's Cyber Security Incident Response Plan.

2.0 REFERENCES

Refer to the main body of this procedure for reference documents.

Where section numbers are referenced within this appendix, the section is local to this appendix unless otherwise specified.

3.0 DEFINITIONS

Refer to the main body of this procedure.

4.0 RESPONSIBILITIES

Refer to the main body of this procedure.

5.0 DETAILS

5.1 Process Overview

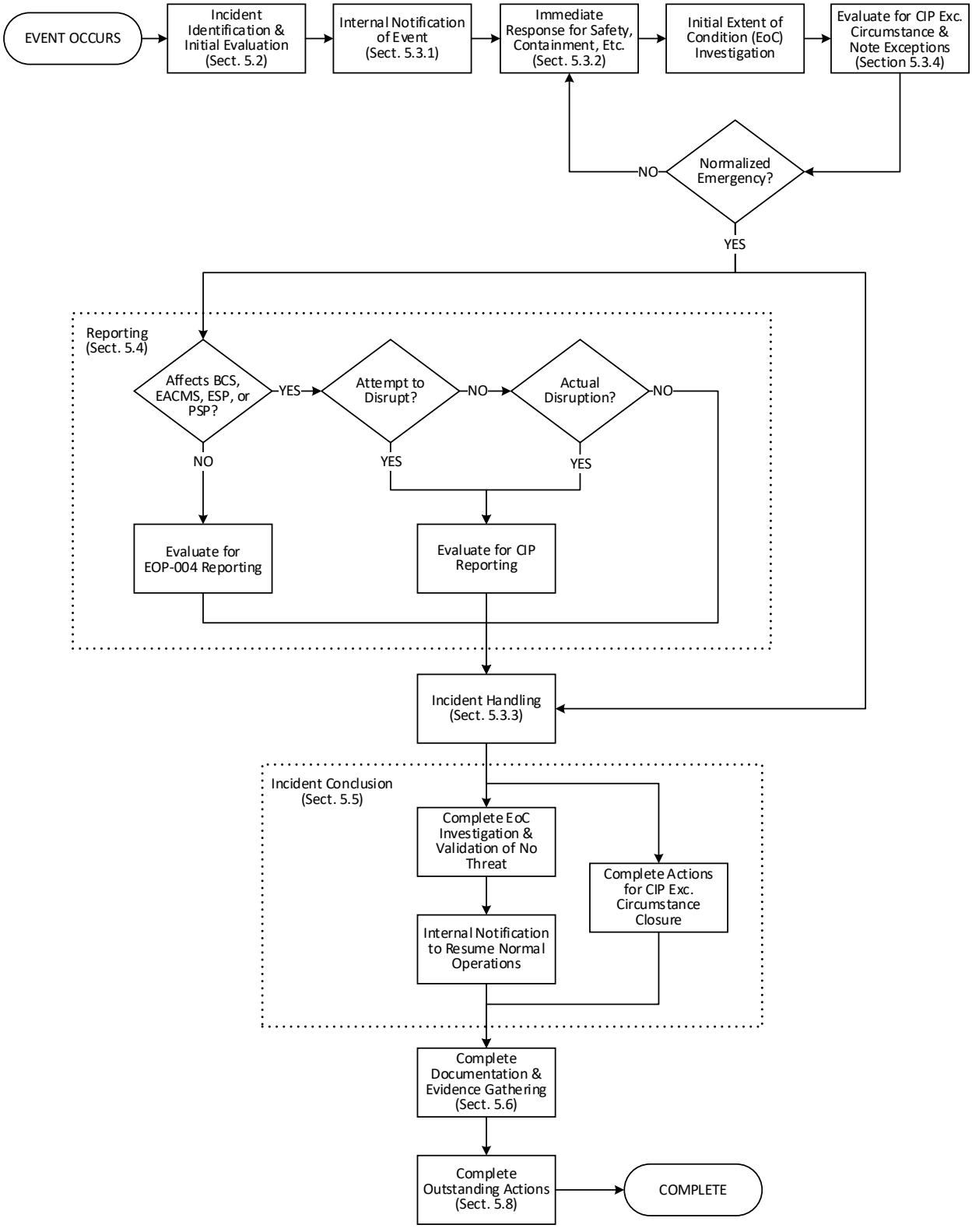
5.1.1 The included flowchart depicts the recommended sequence for incident response activities, also detailed in the subsequent sections. Note that activities may be performed in any order, concurrently, or repeated, as deemed necessary to respond to the situation at hand.

5.1.2 See next page for Incident Response Flowchart.

APPENDIX D

Cyber Security Incident Response

Page 2 of 9



APPENDIX D

Cyber Security Incident Response
Page 3 of 9

5.2 Identification

5.2.1 Personnel and contractors shall notify the Operations Supervisor of any actual or suspected Cyber Security Incidents.

5.2.2 Disruption of a Cyber Asset

5.2.2.1 For NERC CIP applicable Cyber Assets, a disruption is an unplanned event that causes a programmable electronic device to be inoperable. Inoperable is the inability of the programmable electronic device to perform its intended core function, which is based on the reliability tasks in the NERC Functional Model. NERC's definition of Cyber Security Incidents also includes attempts to disrupt a BCS. This equates to the detection of efforts to harm the reliable operation of the BES, which may be precursors to an actual incident.

5.2.2.2 Examples of a disruption include, but are not limited to:

A. Successfully disrupting an Electronic Access Control or Monitoring System from logging or alerting.

B. Successfully disrupting a control system, or components of it, from operating as expected.

5.2.2.3 Examples of an attempt to disrupt include, but are not limited to:

A. Attempts to disrupt Electronic Access Control or Monitoring System logging or alerting by severing a communication line.

B. Attempts to disrupt data exchange by an attempted/unsuccessful Denial of Service (DoS) attack.

5.3 Incident Response

5.3.1 Upon Identification of a Cyber Security Incident (or suspected Incident), the Site's personnel shall immediately report the Incident to the Operations Supervisor and any other appropriate management personnel.

5.3.2 Immediate Response

Note: Some reporting requirements for Cyber Security Incidents are within one (1) hour <u>from the time the Cyber Security Incident is determined to meet a reporting threshold</u>. (Ref. Attachment D1, "Event Reporting Matrix," for time reporting requirements.) It is recommended that incident reporting be assigned to a group or individual that can focus on reporting while other incident response activities take place.

APPENDIX D

Cyber Security Incident Response
Page 4 of 9

5.3.2.1 Asset Manager, Operations Supervisor, *CIP Senior Manager* or delegate, and any appropriate designated personnel shall respond to and mitigate Cyber Security Incidents. Considerations for response include:

A. Stage of the incident (beginning, in-progress, or past)

B. Potential dangers or safety effects on facility operation or personnel

C. Systems and equipment that are or may be affected

D. Availability of backup or redundant systems

E. Who should be involved in the immediate response (e.g., Security, IT, Engineering, Maintenance, etc.)

5.3.2.2 For Cyber Security Incidents, the Operations Supervisor shall contact and coordinate with the Asset Manager and *CIP Senior Manager* or delegate on the appropriate Cyber Security Incident Reporting and Response.

5.3.2.3 For a physical security breach or threat, the Operations Supervisor shall formulate an immediate response that may include:

A. Alerting on-site personnel of any existing safety issues. If the safety of personnel is threatened, personnel may be directed to take refuge or other actions as appropriate.

B. Determining if additional assistance is immediately needed from *local law enforcement* (see Site Data Sheet) and contacting them using either of the methods below:

a. phone 9-1-1

b. phone *See Site Data Sheet.*

C. Taking actions to mitigate the immediate risk to reliable operation of the Bulk Electric System.

5.3.3 Incident Handling

5.3.3.1 The scenarios and actions outlined in this section are not intended to be all-inclusive, and any additional actions are determined by the Asset Manager, Operations Supervisor, and *CIP Senior Manager* or delegate on a case-by-case basis.

5.3.3.2 Breaches

A. Physical Security Perimeter (PSP) Breaches – Physical

APPENDIX D

Cyber Security Incident Response
Page 5 of 9

security breaches should be investigated, and the security perimeter secured. If determined to be a malicious act or potentially malicious act, responses may include:

a. Ensuring the safety of on-site personnel

b. Notifying law enforcement (as appropriate)

c. Determining whether the attack has caused damage to equipment that could compromise or disrupt reliable operations

B. Electronic Security Perimeter (ESP) Breaches – The immediate response should focus on containment of the problem to minimize its effects on equipment and stop the spread to other parts of the system. This may include:

Note: Data preservation should not impede or restrict recovery, but cyber data, such as corrupted drives or recorded data, should, to the greatest extent possible, be preserved for follow-up investigations and full recovery.

a. Disabling connectivity

b. Implementing access restrictions

c. Removing equipment or programs from service (provided its removal does not itself compromise or disrupt stable operations).

d. Requesting technical support as needed (engineering, maintenance, IT) to ensure proper response and to recover BES Cyber System functionality.

5.3.3.3 Attacks

A. Physical Security Perimeter (PSP) attacks – The immediate response should focus on ensuring the safety of on-site personnel and mitigating the risk to reliable operations by protecting, restoring, or securing equipment or by otherwise stabilizing or securing site operations.

B. Electronic Security Perimeter (ESP) attacks – The immediate response should focus on ensuring the ESP is still secure and that the Cyber Attack did not result in an

APPENDIX D

Cyber Security Incident Response
Page 6 of 9

ESP Breach. Responses may include:

a. Reviewing ESP configurations (firewall settings, intrusion detection logs, etc.)

b. Validation that Cyber Assets have not been compromised

c. Requesting technical support as needed (engineering, maintenance, IT) to ensure proper response and to recover BES Cyber System functionality.

5.3.3.4 Threats

A. Verbal Threats – Obtain all available information regarding the threat so that appropriate notifications and actions may begin.

a. If a caller is involved, question them and obtain type of threat and any other available details. Keep on the line as long as possible for tracing purposes (if possible).

b. Notify the Operations Supervisor and other appropriate management so that reporting requirements may be considered.

B. Physical Security Perimeter (PSP) threats (bombs, sabotage, weaponry, etc...) – Conduct a review of protective measures that are in place to ensure mitigation capability is intact.

a. Implement increased security measures such as more frequent security patrols or additional security personnel (as appropriate).

b. Conduct searches of security perimeters and site areas for signs of ingress or attempted ingress and report to the Operations Supervisor and other appropriate management.

c. Once the threat window has passed, consider returning measures and controls to the baseline security posture.

C. Electronic Security Perimeter (ESP) threats – although uncommon, threats to the ESP should be responded to using the same measures above for ESP attacks.

APPENDIX D

Cyber Security Incident Response
Page 7 of 9

5.3.3.5 Suspected Activities

A. All suspected activities should be treated as breaches until investigations have been completed. The Operations Supervisor should be notified of the Suspected Activity. If a suspected PSP/ESP breach is determined to be invalid, normal operations should continue. Suspected Activities may include:

a. Suspicious Activity within or near the Facility

b. Unknown devices, equipment, packages within the Facility

c. Unknown (abnormal) personnel

d. Unexplained equipment malfunctions

e. Abnormal behavior of Cyber Assets

5.3.4 CIP Exceptional Circumstances

5.3.4.1 The Site's shall determine if the incident meets the definition of a CIP Exceptional Circumstance (Ref. SAV-PRO-CIP-003 main body Section 3.0, "Definitions"). If so, the handling of related documentation and activities shall adhere to the requirements defined in SAV-PRO-CIP-003 main body Section 5.4.

5.3.4.2 Actions taken to respond to a CIP Exceptional Circumstance may deviate from previously defined CIP related procedures and/or regulations. Deviations or exceptions to defined procedures should be noted for future review.

5.4 Reporting

5.4.1 Refer to Attachment D1, "Event Reporting Matrix" for guidance on classifying and reporting events.

5.4.2 Reporting methods and contact information are included in Attachment D2, "Reporting Contacts."

5.5 Incident Conclusion

5.5.1 The following items should be considered when determining that response activities may conclude:

5.5.1.1 Safety concerns are no longer imminent

5.5.1.2 Breached perimeters have been secured (may include alternate methods that deviate from normal configuration)

APPENDIX D

Cyber Security Incident Response
Page 8 of 9

5.5.1.3 Affected equipment, systems, and/or structures have been restored to design

5.5.1.4 Tests of restored equipment, systems, and/or structures have been completed as necessary

5.5.2 The Asset Manager, Operations Supervisor, and *CIP Senior Manager* or delegate shall verify with responding groups and individuals that the incident has not expanded to other areas that were not apparent at incident onset and that all detected occurrences have been addressed.

5.5.3 Affected personnel should be notified that the incident has concluded and to resume normal operations.

5.5.4 For events determined to be CIP Exceptional Circumstances, additional actions may be associated with concluding an incident (Ref. SAV-PRO-CIP-003 main body Section 5.4).

5.6 Documentation

5.6.1 Each invocation of this Cyber Security Incident Response Plan, either in response to an actual incident or as a test of this plan, shall be documented. Documentation shall include:

5.6.1.1 Incident details

5.6.1.2 Mitigation and response actions taken

5.6.1.3 Deviations from the plan

5.6.1.4 Lessons learned, or a statement that there were no lessons learned

5.6.1.5 Post-incident analysis

5.6.1.6 Corrective Action Plan including planned future prevention methods

5.6.2 For events determined to be CIP Exceptional Circumstances, additional documentation is required to be retained (Ref. SAV-PRO-CIP-003 main body Section 5.4).

5.7 Implementation and Testing

5.7.1 *CIP Senior Manager* or delegate shall perform a test of this Cyber Security Incident Response Plan (often referred to as a “Cyber Security Incident Response Exercise”) at least once every thirty-six (36) calendar months, by one of the following methods:

5.7.1.1 Responding to an actual Reportable Cyber Security Incident

APPENDIX D

Cyber Security Incident Response
Page 9 of 9

5.7.1.2 Using a drill or tabletop exercise of a Reportable Cyber Security Incident

5.7.1.3 Using an operational exercise of a Reportable Cyber Security Incident

5.8 Updates and Notifications

5.8.1 The Cyber Security Incident Response Plan shall be updated with identified deficiencies corrected and affected personnel notified within 180 days, as applicable, following any of the events listed in Section 5.7 above.

5.8.2 The Cyber Security Incident Response Plan shall be updated, and all affected personnel notified within 60 days of any of the following events:

5.8.2.1 Changes in responsibilities assigned to a group or individual

5.8.2.2 Changes to the inclusion or exclusion of groups or individuals assigned as having responsibilities within the plan

5.8.2.3 Technology changes that would impact execution of the plan

6.0 RECORDS

Refer to the main body of this procedure.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

This appendix is written in accordance with CIP-003-8 Attachment 1 Section 4. Refer to the main body of this procedure and Attachment 1, “Required Sections for Cyber Security Plan(s) for Assets Containing *Low Impact BES Cyber Systems*” for specific requirements.

8.0 KEY WORDS

Refer to the main body of this procedure.

9.0 ATTACHMENTS

9.1 Attachment D1: Event Reporting Matrix

9.2 Attachment D2: Reporting Contacts

ATTACHMENT D1
Event Reporting Matrix

BES Cyber System Impact Rating	Classification / Incident Type	Criteria/Threshold	Form	Time	Reported to:			
Low	Security Breach (physical)	Criterion 1 – Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations.	DOE-417 (notify NERC & E-ISAC in Sect. W), email, or 24-hour incident lines	1 Hour	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Security Breach (cyber)	Criterion 2 – Meets the definition of Reportable Cyber Security Incident (Ref. SAV-PRO-CIP-003 main body Section 3.0, “Definitions”).	(same as above)	1 Hour	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Security Breach (cyber)	Criterion 3 – Cyber event that is not a Reportable Cyber Security Incident that causes interruptions of electrical system operations.	(same as above)	1 Hour	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Security Breach (physical)	Criterion 10 – Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems.	(same as above)	6 Hours	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Security Breach (cyber)	Criterion 11 – Cyber event that could potentially impact electric power system adequacy or reliability.	(same as above)	6 Hours	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Fuel Supply	Criterion 13 – Fuel supply emergencies that could impact electric power system adequacy or reliability. (Fuel supply is typically not considered a Cyber Incident, but is required reporting via DOE-417)	(same as above)	6 Hours	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Security Breach (physical)	Criterion 16 – Damage or destruction of its Facility that results from actual or suspected intentional human action. It is not necessary to report theft unless it degrades normal operation of its Facility.	(same as above)	24 Hours *	DOE	NERC & Region	RC, BA, TOP	E-ISAC
Low	Threat (physical)	Criterion 17 – Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.	(same as above)	24 Hours *	DOE	NERC & Region	RC, BA, TOP	E-ISAC

* By the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM Friday to 8 AM Monday, local time).

ATTACHMENT D1
Event Reporting Matrix

BES Cyber System Impact Rating	Classification / Incident Type	Criteria/Threshold	Form	Time	Reported to:			
Low	Security Breach (cyber, physical)	Information on cyber events have been classified as incidents by your organization not already reported by the DOE-417 form.	E-ISAC portal, email, or 24-hour incident line	5 Business Days *				E-ISAC
Low	Threat (cyber)	Threats received of intended cyber malicious activities (publicly or privately) to either employees or the company.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (cyber)	Data destruction, data theft, or data manipulation/encryption which does not potentially impact electric power system adequacy or reliability.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (cyber)	Other public events such as website defacements, DDoS activity, etc.	(same as above)	5 Business Days *				E-ISAC
Low	Threat (cyber)	Malicious or suspicious email messages and attachments.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (cyber)	Malicious website activity targeting company websites, or websites utilized by electric sector asset owners and operators.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (cyber)	Malicious files or activity associated with removable media.	(same as above)	5 Business Days *				E-ISAC
Low	Threat (cyber)	Other suspicious activity related to electric systems operations technology.	(same as above)	5 Business Days *				E-ISAC
Low	Threat (physical)	Expressed or implied threat – Receipt of verbal or written threat to commit a crime that will result in death or bodily injury to another person(s).	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (physical)	Break-ins/attempted break-ins – Unauthorized personnel attempting to enter or actually entering a restricted area or secured protected site.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (physical)	Tampering or vandalism – Discovery of damage, defacement, or destruction of an Electrical facility/infrastructure or secured protected site which does not have the potential to degrade the normal operation of the Facility.	(same as above)	5 Business Days *				E-ISAC
Low	Security Breach (physical)	Theft, loss, or diversion – Indications of individuals stealing or diverting something associated with a facility/infrastructure or secured protected site.	(same as above)	5 Business Days *				E-ISAC

* No reporting timeframe is prescribed by E-ISAC nor CIP-003. This value is provided as a procedural requirement.

ATTACHMENT D1
Event Reporting Matrix

BES Cyber System Impact Rating	Classification / Incident Type	Criteria/Threshold	Form	Time	Reported to:			
Low	Security Breach (physical)	Social Engineering attempts – Discovery of an individual presenting false information or misusing insignia, documents, identification, etc., to misrepresent affiliation as a means of concealing possible illegal activity. Individuals soliciting information at a level beyond mere curiosity about a public or private event; particular facets of a facility or building, and its purpose, operations, security procedures.	E-ISAC portal, email, or 24-hour incident line	5 Business Days *				E-ISAC
Low	Threat (physical)	Observation, surveillance – Unknown drones flying or hovering over power plants, substations, or transmission lines. Individuals demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest.	(same as above)	5 Business Days *				E-ISAC

* No reporting timeframe is prescribed by E-ISAC nor CIP-003. This value is provided as a procedural requirement.

ATTACHMENT D2
Reporting Contacts

Industry-wide Entities

Department of Energy

- online http://www.oe.netl.doe.gov/oe417.aspx
- email doehqeoc@hq.doe.gov
- fax 202.586.8485 (if e-mail unavailable)
- phone 202.586.8100 (if email/fax unavailable)

Note: Prior to submitting the form to DOE using the online DOE-417 system, respondents are given a choice whether to share information collected on the DOE-417 form with NERC.

Electric Reliability Organization (NERC)

- email systemawareness@nerc.net
- phone 404.446.9780, option 1
- fax 404.446.9770

Electricity Information Sharing and Analysis Center (E-ISAC)

- portal www.eisac.com
- email operations@eisac.com
- malicious code malware@eisac.com (zip files)
- primary phone 202.790.6000
- incident line 404.446.9780, option 2

ATTACHMENT D2
Reporting Contacts

Region-specific Entities

Regional Entity *(MRO)*

- phone 651.855.1753
- phone 651.734.8355 (24-Hour line)
- email events@midwestreliability.org

Regional Entity *(SERC)*

- phone 877.644.7372
- email reporting_line_sit@list-serc1.org

Regional Entity *(RF)*

- phone 216.530.0600
- phone 330.704.0716 (after hours)
- email disturbance@rfirst.org

Regional Entity *(NPCC)*

- phone 212.840.1070
- email event-analysis@npcc.org

Regional Entity *(WECC)*

- phone 801.883.6859
- email disturbancereports@wecc.biz

Regional Entity *(TRE)*

- phone 512.583.4900
- email rapa@texasre.org

Regional Entity *(FRCC)*

- phone 305.442.5748
- email ea@frcc.com

ATTACHMENT D2
Reporting Contacts

Region-specific Entities (continued)

Reliability Coordinator *(SPP)*

- phone 501.614.3900, option 1
- phone 501.804.6580
- email spprcsa@spp.org
- email security@spp.org
- fax 501.482.2031

Reliability Coordinator *(ERCOT)*

- email shiftsupervisors@ercot.com

Note: Typically, the *QSE* and/or *TSP* are obligated to provide required reports to *ERCOT*. (Ref. *ERCOT* Nodal Operating Guide 3.)

Reliability Coordinator *(MISO)*

- email RTOpsCompliance@misoenergy.org

Reliability Coordinator *(CAISO)*

- email erc@caiso.com

Reliability Coordinator *(NYISO)*

- email event-analysis@npcc.org (contact NPCC)

Reliability Coordinator *(RC West – CAISO)*

- phone 916.538.5722
- email rcwest@caiso.com

Reliability Coordinator *(ISO-NE)*

- phone 413.535.4000
- fax 413.535.4379

Note: Where time allows within the reporting time period of the applicable NERC Reliability Standard, in order for ISO to review the validity of the content in the report and its applicability to the Bulk Electric System (BES), Market Participants are encouraged to collaborate with ISO. The preferred means of report submission within the reporting time period shall be by ISO. (Ref. ISO New England Operating Procedure No. 10.)

ATTACHMENT D2 **Page 4 of 4**
Reporting Contacts

Region-specific Entities (continued)

Reliability Coordinator *(FRCC)*

- phone 305.442.5748
- email ea@frcc.com

Reliability Coordinator *(PJM)*

- email dispsup@pjm.com

Note: Specific to the *PJM* Operating Plan, if an event requires a report to be submitted, *PJM* will submit an event report. Member companies are required to provide the event information to *PJM* via the EOP-004 process or the DOE-417 form. Copies of the reports required for EOP-004 are to be provided to *PJM* six (6) hours prior to the twenty-four (24) hour submittal deadline to allow time for *PJM* to meet reporting requirements. (Ref. *PJM* Manual 13.)

Qualified Scheduling Entity (See Site Date Sheet)

- phone *XXX.XXX.XXXX*
- email *yyyy@xxxxxx.com*

Law Enforcement (See Site Data Sheet)

- phone 9-1-1
- phone *XXX.XXX.XXXX*

Note: If the local law enforcement agency decides state or federal agency law enforcement should respond and investigate, the local law enforcement agency should notify and coordinate with those agencies.

APPENDIX E

Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
Page 1 of 4

1.0 PURPOSE

This appendix to procedure SAV-PRO-CIP-003 provides written guidance on how to mitigate the risk of malicious code introduction from Transient Cyber Assets and Removable Media to BES Cyber Systems in compliance with NERC Standard CIP-003.

This appendix serves as the Site's Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation Plan.

2.0 REFERENCES

Refer to the main body of this procedure for reference documents.

Where section numbers are referenced within this appendix, the section is local to this appendix unless otherwise specified.

3.0 DEFINITIONS

Refer to the main body of this procedure.

4.0 RESPONSIBILITIES

Refer to the main body of this procedure.

5.0 DETAILS

5.1 For all Transient Cyber Assets (TCAs) and Removable Media (RM) managed by the Site, the Site personnel shall:

5.1.1 Identify and catalog all TCAs and RM.

5.1.2 Ensure antivirus software is installed on the TCA, that antivirus software definitions remain current, and antivirus scans (or active scans) are scheduled to be performed on a regular basis.

5.1.3 Limit the number of applications allowed to be installed on the TCA as necessary via an Application Whitelisting methodology.

5.2 On-Demand Device Acceptance

5.2.1 Prior to allowing any TCA or RM (owned by the Site or a third party) to be connected to the site's BES Cyber Systems, the Site personnel shall verify one or more of the following via the completion of Attachment E1, "TCA/RM On-Demand Device Acceptance Form." Any system-generated

APPENDIX E

Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
Page 2 of 4

reports (e.g., antivirus scan results) shall also be retained as evidence with the completed form.

Note: If during device verification, the Site personnel determine additional mitigation actions are necessary to ensure cyber security, the Site personnel may implement additional mitigation activities (with the third party's support) or reject the device for use at the facility at their discretion.

5.2.1.1 If antivirus software is installed and implemented on the device, antivirus software definitions are current, and antivirus scans (or active scans) have been performed on the device recently (as appropriate). This may include ensuring that antivirus scans are performed at the time of inspection.

A. For any discovered Malicious Code, the Site personnel shall ensure all threats have been eliminated prior to connection to a BES Cyber System.

5.2.1.2 If application Whitelisting is implemented on the device.

5.2.1.3 If adequate System Hardening is implemented on the device.

5.2.1.4 If a Live Operating System (or software) is implemented on the media and modifications to the code are restricted through the use of Read-Only and Executable Only controls.

5.2.1.5 If any external wireless connectivity (hotspot, Wi-Fi, etc.) is disabled on the device while on site.

5.2.1.6 If the device is incapable of using methods that mitigate the introduction of malicious code (proprietary hand-held devices, etc.).

5.2.1.7 If an alternative method to reduce the risk of Malicious Code is implemented on the device. If so, the Site personnel shall ensure the details of the alternative method are recorded on the TCA/RM On-Demand Device Acceptance Form.

5.2.2 For any Removable Media (RM), if antivirus scans (or active scans) have been performed on the Removable Media recently (as appropriate). This

APPENDIX E

Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
Page 3 of 4

may include ensuring that antivirus scans are performed at the time of inspection.

5.2.2.1 For any discovered Malicious Code, the Site personnel shall ensure all threats have been eliminated prior to connection to a BES Cyber System.

> Note: If antivirus scans are performed by the Site personnel using the Site's Cyber Assets, the Cyber Asset must not be part of any of the Site's BES Cyber Systems (e.g., SCADA, DCS, EMS, etc.).

5.3 Advance Programmatic Acceptance

5.3.1 To allow a specified third-party organization to become exempt from On-Demand Device Acceptance, the Site personnel may review the third party's cyber security policies, procedures, and/or documentation to determine if their implemented processes are acceptable. the Site personnel shall verify one or more of the following processes is enacted by the third party via the completion of Attachment E2, "TCA/RM Advance Programmatic Acceptance Form."

5.3.1.1 If antivirus software is installed and implemented on their devices, antivirus software definitions remain current, and antivirus scans or active scans are performed on the devices regularly.

A. For any discovered Malicious Code, the third party ensures all threats have been eliminated prior to connection to a BES Cyber System.

5.3.1.2 If application Whitelisting practices are implemented on their devices.

5.3.1.3 If adequate System Hardening practices are implemented on their devices.

5.3.1.4 If a Live Operating System or software is implemented on their media and modifications to the code are restricted through the use of Read-Only and Executable Only controls.

5.3.1.5 If their devices are incapable of using methods that mitigate the introduction of malicious code (e.g., proprietary hand-held devices, etc.).

5.3.1.6 If an alternative method to reduce the risk of Malicious Code is implemented on their devices. The Site personnel shall ensure

APPENDIX E

Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
Page 4 of 4

the details of the alternative method are recorded on the TCA/RM Advance Programmatic Acceptance Form.

5.3.1.7 For any Removable Media (RM), if antivirus scans or active scans are performed on the Removable Media regularly.

A. For any discovered Malicious Code, the third party ensures all threats have been eliminated prior to connection to a BES Cyber System.

5.3.2 Approved Advance Programmatic Acceptance Forms expire twelve (12) months after Acceptance Date, at which point, a new review and approval may be performed for a third party to continue using TCAs/RM under Advance Programmatic Acceptance.

6.0 RECORDS

Refer to the main body of this procedure.

7.0 REGULATIONS, STANDARDS, AND REQUIREMENTS

This appendix is written in accordance with CIP-003-8 Attachment 1 Section 5. Refer to the main body of this procedure and Attachment 1, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems” for specific requirements.

8.0 KEY WORDS

Refer to the main body of this procedure.

9.0 ATTACHMENTS

9.1 Attachment E1: TCA/RM On-Demand Device Acceptance Form

9.2 Attachment E2: TCA/RM Advance Programmatic Acceptance Form

ATTACHMENT E1 **Page 1 of 1**

TCA/RM On-Demand Device Acceptance Form

Date	Name and Company

Device Ownership	Device ID/Description
Site Managed ☐ Third Party ☐	

Reason for Connecting

Device Type	Verification Type:
Transient Cyber Asset (e.g., laptop) ☐ Removable Media (e.g., flash drive) ☐	Device Antivirus Levels and Recent Scans verified ☐ Device Antivirus Levels and Recent Scans performed ☐ Device Whitelisting ☐ System Hardening on Device ☐ Device is Live Operating System / Read Only ☐ Device Incapable of Antivirus ☐ Other (describe in 'Comments' below) ☐

Antivirus Installed?	Antivirus Brand	Antivirus Current?	Recent Scan Performed?	Scan Date? (if available)
Yes ☐ No ☐ N/A ☐		Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐	

Malicious Code Detected?	Viruses Quarantined?	Wi-Fi / Bluetooth disabled?	Comments / Additional Mitigations (Describe whitelisting, hardening, live OS, device incapability, or "other method" used on device. Describe any additional mitigations performed?)
Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐	

Device Accepted for Use?	Verification Performed by:	Verifier Signature
Yes ☐ No ☐ N/A ☐		

ATTACHMENT E2

TCA/RM Advance Programmatic Acceptance Form

Third-Party Company		Expiration Date (12 Months from Acceptance Date)	

Transient Cyber Assets

Method Utilized?	For the below primary methods utilized in the mitigation of malicious code within Transient Cyber Assets, one or a combination of selections is acceptable, but one must be selected at minimum. (Cont. on page 2.)	
Yes ☐	**Third party has agreed to primarily use Transient Cyber Assets owned and operated by the facility as capable. For devices owned and operated by the facility, the Site utilizes:**	
	Yes ☐	Antivirus software, including manual or managed updates of signatures or patterns
	Yes ☐	Application Whitelisting
	Yes ☐	Other methods to mitigate the introduction of malicious code (describe):
	Comments:	
Yes ☐	**Third party shall be subject to On-Demand Device Acceptance scanning of Transient Cyber Assets brought to the Site.**	
	Third party has agreed that their Cyber Assets necessary for the performance of in-scope activities will be subject to an On-Demand Device Acceptance scan performed or verified by the Site personnel prior to the device being connect to any BES Cyber Systems owned and operated by the Site. Each scan will be logged on a TCA/RM On-Demand Device Acceptance Form (Ref. Attachment E1). Antivirus system scans may be performed on third-party devices by a device owned by the Site, or self-scan results may be displayed/demonstrated to the Site personnel for verification. If antivirus scans are performed by the Site personnel using the Site Cyber Assets, the Cyber Asset must not be part of the Site's BES Cyber System (e.g., SCADA, DCS, EMS, etc.), but may be a stand-alone device or a device used on their business, corporate, or other administrative network.	
	Comments:	
Yes ☐	**The Site has confirmed that some third party's devices do not have capabilities to use methods that mitigate the introduction of malicious code (incapable of antivirus install, etc.). Please list incapable devices owned by third party below and general reason for incapability, attaching additional pages as necessary. Retain supporting evidence documenting incompatibility with this completed form.**	
	Device	**Reason**
	Comments:	

ATTACHMENT E2

TCA/RM Advance Programmatic Acceptance Form

Third-Party Company		Expiration Date	

Transient Cyber Assets (cont.)

Method Utilized?	For the below primary methods utilized in the mitigation of malicious code within Transient Cyber Assets, one or a combination of selections is acceptable, but one must be selected at minimum.	
Yes ☐	**The Site has reviewed and verified the third party's methods and processes for malicious code mitigation and accepted the third party's use of Transient Cyber Assets (TCA) at the facility. The processes utilized by the third party are sufficient to allow Cyber Assets owned, operated, and managed by the third party to be connected to BES Cyber Systems owned and operated by the Site. The methods utilized help prevent the introduction of malicious code or other damaging software by the third party's TCAs (capable of transmitting or transferring executable code) that are necessary for the performance of in-scope activities. This applies to devices intended to be directly connected (e.g., via cabling, Wi-Fi, or any other method) to BES Cyber Systems owned and operated by the facility. One or a combination of the following processes or methods listed below is utilized by the third party and strictly enforced for all personnel and any hired subcontractor party personnel.**	
	Yes ☐	Antivirus Update Process: For all devices capable, the third party maintains current antivirus and malicious code prevention software on their devices that is kept up-to-date, has current definitions, and performs full system scans on a regular basis. For any device found by the third party to contain malicious code or damaging software, the third party takes appropriate steps to quarantine, isolate, or eradicate all discovered abnormalities and threats prior to returning the device into service for field work and subsequent connection to the facility's BES Cyber System. Furthermore, the third party agrees that their devices will be subject to On-Demand Device Acceptance spot checks / verifications at the discretion of the Site to ensure the above stated practices are being executed.
	Yes ☐	Application Whitelisting: The third party maintains a whitelist methodology for their field devices intended to be connected to BES Cyber Systems which only allows approved and limited applications to be installed on the cyber asset that are necessary for the performance of in-scope activities.
	Yes ☐	Live Operating System and Software Executable only from read-only media: Third party maintains operating systems and executable software on separate isolated storage devices (e.g., thumb drives, etc.) in order to mitigate the introduction of malicious code within the OS or software. Facility personnel should review the third party's processes to build the read-only media as possible.
	Yes ☐	System Hardening: Third party maintains a combination of system hardening methodologies on their field device which may include port closures, spyware protection, encryption, logical access controls, antivirus, default setting adjustments, security patches update processes, elimination of unused features, etc. in order to mitigate the introduction of malicious code on their device.
	Yes ☐	Third party utilizes other methods to mitigate the introduction of malicious code (describe):
	Comments:	

ATTACHMENT E2
TCA/RM Advance Programmatic Acceptance Form

Third-Party Company		Expiration Date	

Removable Media

Method Utilized?	For the below methods utilized in the mitigation of malicious code within Removable Media, one or a combination of selections is acceptable, but one must be selected at minimum.	
Yes ☐	**Third party shall be subject to On-Demand Device Acceptance scanning of all Removable Media brought to the Site.**	
	Yes ☐	Third party has agreed that their Removable Media necessary for the performance of in-scope activities will be subject to an On-Demand Device Acceptance scan performed or verified by the Site personnel prior to the device being connect to any BES Cyber Systems owned and operated by the Site. Each scan will be logged on a TCA/RM On-Demand Device Acceptance Form (Ref. Attachment E1). Antivirus system scans may be performed on third-party media by a device owned by the Site. If antivirus scans are performed by the Site personnel using the Site Cyber Assets, the Cyber Asset must not be part of the Site's BES Cyber System (e.g., SCADA, DCS, EMS, etc.), but may be a stand-alone device or a device used on their business, corporate, or other administrative network.
	Comments:	
Yes ☐	**The Site has reviewed the third party's method of malicious code mitigation for their Removable Media and approved the third party's use of Removable Media at the facility.**	
	Yes ☐	The Site has verified that processes are utilized by the third party to detect the introduction of malicious code on their Removable Media and that all detected threats are mitigated prior to the device being connect to any BES Cyber Systems owned and operated by the Site.
	Comments:	

Third-Party Contact Information

Contact Person's Name & Title	
Contact Phone	
Contact Email	

Approval

By signing below, the Transient Cyber Assets and Removable Media owned and operated by the third party have been accepted for use at the Site per the above-described methodologies for mitigating the introduction of malicious code into the Site's BES Cyber Systems. the Site still reserves the right to reject the use of third-party Transient Cyber Assets or Removable Media at any time.

Acceptor's Name & Title	

Acceptor's Signature	Acceptance Date