CIP 007 -5

Transition to Version 5

Val Ayers
NPCC Lead CIP Auditor
### Version 8

#### 10.3.2.1 Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more document processes that collectively include each of the applicable requirement parts in OP-007-9 Tables 9-10: Ports and Services.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the responsible entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports are open by default.

2. On a daily basis, defend against the use of unnecessary shutdown input/output ports used for network connectivity, console commands, or removable media.

3. Security Patch Management: The responsible entity shall document and implement a security patch management process that includes identifying, evaluating, and installing applicable security patches for applicable cyber assets within the electronic security perimeter(s).

#### 10.3.2.2 Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more document processes that collectively include each of the applicable requirement parts in OP-007-9 Tables 7-8: Malicious Code Prevention.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Deploy anti-malware tools, data, data, or on-prem malicious code.

2. Mitigate the threat of detected malicious code.

3. For those systems identified in Part 10.3.2.2 that use signature or pattern, have a process for the updating of the signature or pattern. The process must address testing and installing the signature or pattern.

#### 10.3.2.3 Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more document processes that collectively include each of the applicable requirement parts in OP-007-9 Table 6: Security Event Monitoring.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Log events at the RIT Cyber System level (per RIT Cyber System capability) or at the Cyber Asset level (per Cyber asset capability) for identification of, and after-the-fact investigation of, cyber security incidents that include, as a minimum, each of the following types of events:

2. Detect and respond to, or other logical network accessible ports that have been determined to be needed by the responsible entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports are open by default.

3. On a daily basis, defend against the use of unnecessary shutdown input/output ports used for network connectivity, console commands, or removable media.

4. Security Patch Management: The responsible entity shall document and implement a security patch management process that includes identifying, evaluating, and installing applicable security patches for applicable cyber assets within the electronic security perimeter(s).

5. Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the responsible entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports are open by default.

6. On a daily basis, defend against the use of unnecessary shutdown input/output ports used for network connectivity, console commands, or removable media.

7. Deploy anti-malware tools, data, data, or on-prem malicious code.

8. Mitigate the threat of detected malicious code.

9. For those systems identified in Part 10.3.2.2 that use signature or pattern, have a process for the updating of the signature or pattern. The process must address testing and installing the signature or pattern.

10. Log events at the RIT Cyber System level (per RIT Cyber System capability) or at the Cyber Asset level (per Cyber asset capability) for identification of, and after-the-fact investigation of, cyber security incidents that include, as a minimum, each of the following types of events:

11. Detect and respond to, or other logical network accessible ports that have been determined to be needed by the responsible entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports are open by default.

12. On a daily basis, defend against the use of unnecessary shutdown input/output ports used for network connectivity, console commands, or removable media.

13. Deploy anti-malware tools, data, data, or on-prem malicious code.

14. Mitigate the threat of detected malicious code.
### Northeast Power Coordinating Council, Inc.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>4.2 Generate alerts for security events that the Responsible Entity determines necessary, an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or ESI Cyber System capability):</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>MC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.3.1 Detected malicious code from Part 4.2; and 4.3.2 Detected failure of Part 4.1 event logging.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.8A</td>
<td>4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under DP Exceptional Circumstances.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.8B</td>
<td>4.4 Review and summarization of sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undesired Cyber Security incidents.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.9</td>
<td>Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects vulnerabilities, one or more documented processes that collectively include each of the applicable requirement parts in DNP-009-1 Table E5 — System Access Control.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td></td>
<td>5.1 Use a methodology to enforce authentication of interactive user access, where technically feasible.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td></td>
<td>5.2 Identify and inventory all known enabled default or other generic account types, either by system, by group of systems, by location, or by system type(s).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.10</td>
<td>5.3 Identify individuals who have authorized access to shared accounts.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td></td>
<td>5.4 Change known default passwords, per Cyber Asset capability.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.11</td>
<td>5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td></td>
<td>5.5.2 Minimum password complexity that is the lesser of three or more different character types (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td>401-5.12</td>
<td>5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
<tr>
<td></td>
<td>5.7 Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>MC</td>
</tr>
</tbody>
</table>

**R5.3.** The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CP-003-3.

**R5.4.** The Responsible Entity shall retain all logs specified in Requirement 5.3 for ninety calendar days.

**R5.5.** The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

---

3/25/2015
What Changed?

**CIP 007 V3a System Security Management**
- R1 Test Procedures
- R2 Ports and Services
- R3 Security Patch Mgt.
- R4 Malicious Software Prevention
- R5 Account Management
- R6 Security Status Monitoring
- R7 Disposal or Redeployment
- R8 Cyber Vulnerability Assessment
- R9 Documentation Review and Maintenance

**CIP 007 V5 Systems Security Management**
- CIP 010-1 R1 Configuration Change
- CIP 007-5 R1 Ports and Services
- CIP 007-5 R2 Security Patch Mgt.
- CIP 007-5 R3 Malicious Code Prevent
- CIP 007-5 R5 System Access Control
- CIP 007-5 R4 Security Event Monitor
- CIP 011-1 R2 Reuse and Disposal
- CIP 010-1 R3.1 VA
- CIP 010-1 R1 Configuration Change
CIP 006-3 and CIP 005-3
Spider Requirements

CIP 006-3 R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

CIP 005-3 R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.
Part 1 Requirement

1.1
If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

1.2
Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.

Evidence
An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Guidelines and Technical Basis
This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent.
CIP 007-5

Ports and Services

Guidelines and Technical Basis

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset’s configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks
Lessons Learned

Question
Signage for physical port protection (CIP-007-5, R1.2) – is it acceptable to place signs at the PSP doors, rather than on each individual device port?

Response
The preferred method of securing the ports is logically disabling the port. If that is not feasible, then the use of port locks should be used.
If none of the above are used, then the sign (in the appropriate language for the Responsible Entity) should be as close to the applicable port as possible to be effective to deter inappropriate use of the port.
Signage is explicitly allowed as a measure of compliance.
If signage is used, it is recommended that entities develop a process addressing the signage’s content and strategic placement at the PSP perimeter.
Lessons Learned

Question
How can tamper tape be used to protect physical ports to comply with this requirement?

Response
Installing tamper tape over a physical port and recording the serial number or signing the tape can provide visual after-the-fact evidence that a port has been accessed (a detective control). While not preventative in nature, it provides more evidence than either a warning sign (even if attached to a dummy plug placed in the physical port) or physical port blocks that can be removed using a special tool but without a trace that the port block device has been removed. Note that while tamper tape and other similar methods of signage do not prevent unauthorized personnel from accessing these ports, they can be a useful part of a defense-in-depth type of control to remind and deter personnel from unauthorized use of the physical ports.
CIP 007-5 R2 Security Patch Management

Evidence
An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

Guidelines and Technical Basis
The SDT’s intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; the main intention is to “be aware of in a timely manner and manage all known vulnerabilities” requirement.

Part 2.1
A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
Part 2.2
At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

Evidence
An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.
Guidelines and Technical Basis

2.2

Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.
Guidelines and Technical Basis

2.2

The Responsible Entities can use the information provided in the Department of Homeland Security “Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems” as a source. The DHS document “Recommended Practice for Patch Management of Control Systems” provides guidance on an evaluative process.
For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches; or
- Create a dated mitigation plan; or
- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.
Guidelines and Technical Basis

2.3

Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.
CIP 007-5 R2 Security Patch Management

Evidence
An example of evidence may include, but is not limited to, records of implementation of mitigations.

Guidelines and Technical Basis
Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan.

In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Part 2.4
For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
FAQ

Question
Do assets in use for years (e.g. relays installed 6 years ago) have to be current with security patches and does every security patch in history for the device need to be documented. If not how far back does an entity need to go?

Response
For any system’s initial evaluation for security patch evaluation the evaluation must look back at all applicable security patches for that system.

All applicable security vulnerabilities associated with the previously available security patches must be addressed for the scope of the Cyber Asset’s system(s) development life cycle or a mitigation plan must be created.
Questions

• Also, for Medium BES Cyber systems that are brought into scope with CIPv5, how back from the April 2016 implementation deadline would we have to demonstrate the evaluation of historically released patches?

• Response
For any system’s initial evaluation for security patch evaluation the evaluation must look back at all applicable security patches for that system.
All applicable security vulnerabilities associated with the previously available security patches must be addressed for the scope of the Cyber Asset’s system(s) development life cycle.
Questions

- CIP-007 R2 - What will be the expectation for BES Cyber Systems and BES Cyber Assets that have legacy operating systems for which a patch source no longer exists (e.g. Microsoft XP)?

- Response
For any system’s initial evaluation for security patch evaluation the evaluation must look back at all applicable security patches for that system.
All applicable security vulnerabilities associated with the previously available security patches must be addressed for the scope of the Cyber Asset’s system(s) development life cycle.
Questions

• CIP 007 R2 – security patch management: How can we address this requirement on operational assets such as relays? There are no “patches” for these devices. Patches are applicable to computer systems.

• Response

“The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product”
Questions

• How do we handle devices where the OS is not documented by the vendor and is only firmware updatable? We have a lot of IP cameras and other PACS devices that fit this description?

• Response

“A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset’s baseline.”
CIP 007-5 R3 Malicious Software Prevention

Evidence
An example of evidence may include, but is not limited to, records of the Responsible Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

Part 3.1
Deploy method(s) to deter, detect, or prevent malicious code.
Part 3.2
Mitigate the threat of detected malicious code.

Evidence
- Records of response processes for malicious code detection
- Records of the performance of these processes when malicious code is detected.
CIP 007-5 R3 Malicious Software Prevention

Evidence
An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Part 3.3
For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.
Guidelines and Technical Basis

3.1

If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc.
Guidelines and Technical Basis

3.2

When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code.

In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset.
Guidelines and Technical Basis

3.3

Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.
FAQ

Question
For CIP-007-5 R3 Part 3.1 on malicious code for non-routable sites, is hardening or group policy sufficient?

Response
“System hardening", "policies", etc. have been provided as examples of acceptable measures of meeting the requirement to "deploy method(s) to deter, detect, or prevent malicious code". While these methods are defined as acceptable, they should be documented in such a way to demonstrate their applicability to the desired BES Cyber Systems and their ability to provide the required control.
FAQ

Question
For the implementation of malicious code prevention, should entities choose to deter, detect, or prevent malicious code? If an entity chooses to deter, how should they plan on complying with CIP-007-5, R3, Part 3.2 since there would be no mechanism to detect? Is there an implicit requirement in Part 3.2 to deploy detective controls?
FAQ

Response
Part 3.2, in and of itself, does not have an implicit requirement to deploy detective controls; rather, Part 3.2 works in concert with other CIP requirements, such as CIP-007-5, R4, Part 4.1.3 which requires logging for malicious code.
Under Part 3.2, the entities have an obligation to mitigate malicious code whenever it is detected through any means.
Responsible Entities have asked what the relationship is between Part 3.1 and Part 3.2. Whereas Part 3.1 gives Responsible Entities the choice of deploying deterrence, detective, or preventive controls, Part 3.2 simply states detected malicious code must be mitigated.
The goal of Part 3.2 was to get entities to mitigate malicious code when they find it.
Questions

• Serial Device:
  • How do I perform on a serial device a way to deploy method(s) to deter, detect, or prevent malicious code? If it is not technically feasible, what other compensating controls has the Transition Team seen used by industry. How do I need to document this?

• Response
  “There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc.”
Questions

• CIP 007 R3 – Malicious Code prevention: How can we address this requirement on operational assets (OT) such as relays? There is no antivirus for relays. Programs cannot be installed in relays and many other OT assets.

• Response

“If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.”
CIP 007-5 Security Event Monitoring

Evidence

Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

Part 4.1

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;
4.1.2. Detected failed access attempts and failed login attempts;
4.1.3. Detected malicious code.
CIP 007-5 Security Event Monitoring

Evidence
Examples of evidence may include, but are not limited to, paper or system generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

Part 4.2

Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

4.2.1. Detected malicious code from Part 4.1; and
4.2.2. Detected failure of Part 4.1 event logging
Part 4.3

Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.
CIP 007-5 Security Event Monitoring

Evidence
Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Part 4.4
Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
Guidelines and Technical Basis

4.1

This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include:

(i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.
Guidelines and Technical Basis

4.1

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.
Guidelines and Technical Basis

4.2

The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy
Questions

• CIP 007 R 4.1 – OT assets like relays cannot detect successful login attempt or malicious code. How can this requirement be addressed on OT assets?

• Response
  
  • Front end Servers used to authenticate and allow access to assets some times have this capability.
Part 5.1

Have a method(s) to enforce authentication of interactive user access, where technically feasible.

****Applicable Systems ****
Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
1. EACMS;
2. PACS; and
3. PCA
TFE Available ***
Part 5.2

Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
CIP 007-5 System Access Control

Evidence
An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

Part 5.3
Identify individuals who have authorized access to shared accounts.

****Applicable Systems****
Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
1. EACMS;
2. PACS; and
3. PCA
CIP 007-5 System Access Control

Evidence
Examples of evidence may include, but are not limited to:
• Records of a procedure that passwords are changed when new devices are in production; or
• Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

Part 5.4
Change known default passwords, per Cyber Asset capability.
CIP 007-5 System Access Control

Evidence
Examples of evidence may include, but are not limited to:
• System-generated reports or screen-shots of the system enforced password parameters, including length and complexity;
or
• Attestations that include a reference to the documented procedures that were followed.

Part 5.5
For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and

5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.
Question

• What are the areas in CIP that could be met using attestations? Password Changes, Security Patches, Baseline Configurations, etc.

• Response

• See evidence section previous slide and next slide
CIP 007-5 System Access Control

Evidence
Examples of evidence may include, but are not limited to:
• System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or
• Attestations that include a reference to the documented procedures that were followed.

Part 5.6
Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

***Applicable Systems***
Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
1. EACMS;
2. PACS; and
3. PCA
Part 5.7
Where technically feasible, either:

- Limit the number of unsuccessful authentication attempts; or
- Generate alerts after a threshold of unsuccessful authentication attempts.

TFE Available
The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.
Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.
Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.
Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account.

Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.
Questions?