

Standard Application Guide

CIP-010-2

Requirements R1 and R2

June 18, 2020



**MIDWEST
RELIABILITY
ORGANIZATION**

380 St. Peter St, Suite 800
Saint Paul, MN 55102

651-855-1760

MRO.net

TABLE OF CONTENTS

TABLE OF CONTENTS	2
DISCLAIMER	4
INTRODUCTION	5
PREFACE	6
OVERVIEW	7
METHODOLOGY	7
COMMON TERMS AND DEFINITIONS	8
STRUCTURE, FORMAT, & CONTENT	9
EVALUATING CIP-010-2, REQUIREMENT R1, Part 1.1. – 1.5.	11
CIP-010-2 Requirement R1 - Configuration Change Management	15
Analysis, Part 1.1. – Developing Baselines.....	15
CIP-010-2, Requirement R1, Part 1.1 – Developing Baselines	21
Analysis, Part 1.1.1. – Operating System or Firmware Versions.....	21
CIP-010-2, Requirement R1, Part 1.1. – Developing Baselines	26
Analysis, Part 1.1.2. – Installed Commercial or Open-source Software.....	26
CIP-010-2, Requirement R1, Part 1.1. – Developing Baselines	30
Analysis, Part 1.1.3. – Installed Custom Software	30
CIP-010-2, Requirement R1, Part 1.1. – Developing Baselines	35
Analysis, Part 1.1.4. – Logical Network Accessible Ports.....	35
CIP-010-2, Requirement R1, Part 1.1. – Developing Baselines	42
Analysis, Part 1.1.5. – Applied Security Patches	42
CIP-010-2, Requirement R1 – Configuration Change Management	48
Analysis, Part 1.2. – Authorizing & Documenting Baseline Deviations	48
CIP-010-2, Requirement R1 – Configuration Change Management	57
Analysis, Part 1.3. – Updating Baselines	57
CIP-010-2, Requirement R1 – Configuration Change Management	63
Analysis, Part 1.4. – Assessing and Testing Cyber Security Controls	63
CIP-010-2, Requirement R1 – Configuration Change Management	73
Analysis, Part 1.5. – Testing High Impact Baseline Changes.....	73
CIP-010-2, Requirement R2 – Configuration Monitoring	79
Analysis, Requirement R2. Configuration Monitoring	79
CIP-010-2, Requirement R2 – Configuration Monitoring	89
Analysis, Part 2.1 – Monitoring Baselines for Unauthorized Changes	89



MITIGATING RISK AND INTERNAL CONTROLS	97
APPENDIX A: REFERENCES	98
APPENDIX B: ACRONYM GUIDE	99
APPENDIX C: Global Evidence Considerations	101
APPENDIX D: Supporting Analysis; Assessing & Testing	103
APPENDIX E - Governance, Self-Monitoring, & Reasonable Assurance Options	121
Example A: Primary Control (Key Control).....	126
Example B: Secondary Control	128
Example C: Tertiary Control	129
Exhibit A: Requirement R1, Configuration Change Management (3rd Party Tool Options)	133
Exhibit B: Part 1.1 – Establishing Baselines (Manual Options)	134
Exhibit C: Part 1.1.1. – Operating System or Firmware Versions (3rd Party Tool Options)	136
Exhibit D: Part 1.1.1. – Operating System or Firmware Versions (Manual Options)	137
Exhibit E: Part 1.1.2. & 1.1.3 – Commercial, Open-source, or Custom Software (3rd Party Tool Options)	138
Exhibit F: Part 1.1.2. & 1.1.3 – Commercial, Open-source, or Custom Software (Manual Options) .	140
Exhibit G: Part 1.1.4. – Logical Network Accessible Ports (3rd Party Tool Options)	142
Exhibit H: Part 1.1.4. – Logical Network Accessible Ports (Manual Options)	143
Exhibit I: Part 1.1.5. – Applied Security Patches (3rd Party Tool Options)	146
Exhibit J: Part 1.1.5. – Applied Security Patches (Manual Options)	147
Exhibit K: Part 1.2. – Authorizing & Documenting Baseline Deviations (3rd Party Tool Options) ...	148
Exhibit L: Part 1.2. – Authorizing & Documenting Baseline Deviations (Manual Options)	149
Exhibit M: Part 1.3. – Updating Baselines (Manual Options)	151
Exhibit N: Part 1.4. – Assessing and Testing Cyber Security Controls (3rd Party Tool Options)	152
Exhibit O: Part 1.4. – Assessing and Testing Cyber Security Controls (Manual Options)	153
Exhibit P: Part 1.5. – Testing High Impact Baseline Changes (Manual Options)	154
Exhibit Q: Part 2.1 – Monitoring Baselines for Unauthorized Changes (3rd Party Tool Options)	155



DISCLAIMER

The Midwest Reliability Organization (MRO) Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging Reliability Standards. Any materials, including presentations, were developed through the MRO CMEPAC by Subject Matter Experts (SMEs) from member organizations within the MRO region.

SMEs in the field of Critical Infrastructure Protection and Cybersecurity were brought together to prepare a guide for complying with NERC Reliability Standard CIP-010-2 Requirements R1 and R2 (Configuration Change Management & Configuration Monitoring). Participants include representatives from Balancing Authorities (BAs), Distribution Providers (DPs), Resource Planners (RPs), and Generator Owners (GOs). Generator Operators (GOPs), Planning Authorities/Planning Coordinators (PAs/PCs), Transmission Owners (TOs), Transmission Operators (TOPs), Transmission Planners (TPs) and Transmission Service Providers (TSPs).

CIP-010-2 Application Guide – Development Team Subject Matter Experts

Sharon Koller, Chair
American Transmission Company

Daniel Graham, Vice Chair
Basin Electric Power Cooperative

John Chang
Manitoba Hydro

Ronald Bender
Nebraska Public Power District

Lori Frisk, Committee Liaison
Minnesota Power/ALLETE

Francois Yang
Alliant Energy

Terry Jones
Lincoln Electric System

The materials have been reviewed by MRO staff and provide reasonable application guidance for the standard(s) addressed. Ultimately, demonstrating compliance depends on a number of factors including the precise language of the standard, the specific facts and circumstances, and quality of evidence.

These documents may be reproduced or distributed to any person or entity only in its entirety.

The MRO SME Team is an industry stakeholder group which includes subject matter experts from MRO member organizations in various technical areas. Any materials, guidance, and views from stakeholder groups are meant to be helpful to industry participants; but should not be considered approved or endorsed by MRO staff or its board of directors unless specified.



INTRODUCTION

NERC Reliability Standard CIP-010-2 (Cyber Security — Configuration Change Management and Vulnerability Assessments) serves an important purpose by requiring users, owners and operators to implement necessary security controls.

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements to protect BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Applicability:

4.1 Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner



PREFACE

The scope of this Standard Application Guide (SAG) encompasses two Requirements and 13 Requirement Parts. The Standard provides flexibility for Registered Entities to implement a mix of manual and automated options to collectively achieve compliance with CIP-010-2 Requirements R1 - R2 and its 13 Requirement Parts.

Because no two Registered Entities are identical, needs may vary based on factors like, but not limited to, an organization's size, maturity, technology, limited resources, and/or CIP Standards applicability based on functional registration. The Critical Infrastructure Protection Subject Matter Expert Team (CIP SMET) is mindful that a one-size-fits-all approach cannot scale for an industry with diverse infrastructure and myriad implementations, so this SAG is designed to offer a comprehensive body of documented options, examples, and tools to aid the industry in achieving and maintaining compliance in a manner suited to each unique entity.

For each Requirement and Requirement Part, the SAG provides general option-agnostic guidance supplemented by two potential option categories; 1) technology-based approaches leveraging the use of 3rd Party Tools, and 2) manual approaches. As needed, this construct also allows Registered Entities to right-size implementation to their organization by designing hybrid solutions that blend these approaches.

To accomplish this, the CIP SMET designed this SAG with modularity in mind. End-user friendliness was also a significant consideration. While Registered Entities who seek guidance on the full breadth of Configuration Change Management requirements may read this SAG in its entirety for a holistic perspective, that may not be the typical use for this SAG.

Registered Entities who have a more narrowly focused need can navigate to a specific section of content with the comfort that each piece is modular and complete. Because each section's content can be read and applied in a standalone manner, some content may be repeated in its entirety where it is applicable to more than one option for a Requirement or Requirement Part.

The CIP SMET considered removing repeated content and relying on hyperlinks or references to the section where it first appeared and decided this approach would bounce the reader around in between sections creating the potential for confusion for the end user. Rather than compromise the quality of the end-user-experience, or risk the user inadvertently reading content out of context or applicable to the wrong Requirement or Requirement Part, the CIP SMET chose to limit hyperlinking in favor of keeping contiguous content or footnotes where it significantly contributed to the completeness and accuracy of each section. This thoughtful approach assures that relevant and complete information is at the fingertips of each user based on the unique needs and focus areas of that Registered Entity.



OVERVIEW

Multiple methods can meet compliance and security requirements, so Registered Entities should select the best course for their organization. Below is a list of considerations for determining the best course:

- What are the impact ratings?
- Should one solution be used for all systems and impact ratings?
- Is there an existing solution?
- What type of connectivity do the Cyber Assets have?
- How many employees are required to perform the tasks?

METHODOLOGY

To develop implementation guidance with a holistic approach to Critical Infrastructure Protection in the domain of Change Control and Configuration Management, the SME Team that developed this SAG leveraged several methodologies, industry practices, and/or frameworks such as:

- [COBIT](#) (Control Objectives for Information and Related Technologies)
- [ITIL](#) (Information Technology Infrastructure Library)
- [NIST](#) (National Institute of Standards and Technology)
- [CIS](#) (Critical Security Controls) for Security Controls for Effective Cyber Defense
- [OODA](#) (Observe, Orient, Decide, Act) Loop
- [C2M2](#) (Cybersecurity Capability Maturity Model)
- [COSO](#) (Committee of Sponsoring Organizations) of the Treadway Commission
- [IIA](#) (The Institute of Internal Auditors)

These frameworks serve as examples of optional tools or methods that can be used in any combination, and adapted to a Registered Entity's organizational structure, culture, maturity, existing technology or process, and operational programs and practices.

These methods also represent the intended best practices and tools leveraged by members of the CIP-010-2 Subject Matter Expert (SME) Team when designing and implementing Configuration Change Management programs and solutions that achieve and maintain compliance within their organizations.

These methodologies can also serve to aid in a Registered Entity's self-assessment of program maturity and the development of an internal controls program. Internal controls Risk and Control Matrices accompanied by testing plans and a testing schedule is one approach that, if operationalized, has the potential to accomplish continuous monitoring, observational discoveries of potential gaps or deficiencies that pose risk, and opportunity to recommended improvement activities. This may serve to provide reasonable assurance of a Registered Entity's compliance with the mandatory Reliability Standards.



COMMON TERMS AND DEFINITIONS

Please refer to the [NERC Glossary of Terms](#) for authoritative Terms and Definitions.

The following general or common terminology used within this SAG does not replace nor supersede authoritative Terms and Definitions and is intended to provide reasonable meaning and understanding for users of this guide. The MRO Subject Matter Expert Team's goal was to provide comprehensive materials, guidance, and views by offering reasonable ideas, conditions, or use cases; however, where lists, samples, or examples are used they are not to be interpreted as prescriptive nor all inclusive, and other viable outputs or scenarios could exist.

System-generated Evidence: *System-generated* evidence is a generic term used to represent a broad range of potential ways to prove how a system is technically configured, and its actual state on demand or at a point in time. Types of *system-generated* evidence may include, but are not limited to, exports/extracts from a Cyber Asset; reports generated from a querying tool or scan; in system database objects, log records, alert or version history etc.; command outputs saved or captured to a file; screenshots of in-system data or photographs of screens or displays. *System-generated* evidence would not include any manually prepared narratives, lists, or other such documents, although ReadMe type files may certainly be used to help explain the technical contents of *system-generated* evidence.



STRUCTURE, FORMAT, & CONTENT

The CIP SME Team developed a standardized structure for the content of this guide. This approach is intended to aid industry users in quickly navigating to relevant information while providing assurance implementation guidance is in a comprehensive and consistent format. The below table outlines the structure used and provides field descriptors for the type of content to expect in each section.

Requirement Language:	
A citation of the exact language from the CIP-010-2 Requirement or Requirement Part. This provides the needed context for the SME Team's <i>Evaluation</i> that follows in each section.	
Evaluation	
Objective:	Intended to describe the objective of each Requirement or Requirement Part and provide a high-level statement about what it accomplishes. An objective-based approach to implementation guidance helps frame the conversation around minimum mandatory obligations while setting a basis for why compliance with the cited requirement is important.
Value Proposition:	Intended to describe the benefits of meeting the stated objective. An understanding of how compliance with the Requirement or Requirement Part offers added business and operational value that helps align the industry on the importance of cybersecurity standards and our collective goal to deliver safe, secure, resilient, and reliable operation of the BES.
Recommended Application Guidance – Potential Approaches	
The SME Team's narrative analysis of the Requirement Language, Objective, and Value Proposition intended to offer several potential approaches a Registered Entity may consider when determining how to achieve and maintain compliance with mandatory obligations. May also include recommendations for compliance implementation supported by real world experiences, practical knowledge, or plausible scenarios. Intended to deliver a comprehensive collection of potential options to aid Registered Entities in identifying and implementing a right-sized solution commensurate with risk and in alignment with Registered Function(s), asset base, resource model, process/system maturity, and culture of each unique organization.	
Tip:	Intended to advise on various considerations that may minimize compliance and/or security risk, offer mechanisms that deliver efficiency gains, and/or offer creative ideas or alternatives to traditional approaches. Sharing collective experience with diverse implementations by making valuable process or technology tips and tricks available to the industry serves to further position Registered Entities for success in their program design and implementation.
Lessons Learned:	Intended to include practical lessons learned and potential options for consideration to help detect, deter, prevent, respond, and/or recover from certain implementations that may cause unintended consequences, potential non-compliance, or an inability to generate evidence to sufficiently demonstrate compliance. Providing real world experiences and solutions from unexpected situations affords the industry an opportunity to avoid mistakes that others have experienced, thereby increasing success in meeting mandatory obligations.



Recommended Application Guidance – Potential Approaches (continued)	
Evidence:	<p>Intended to support the measures as stated in each Requirement or Requirement Part while also providing options for:</p> <ul style="list-style-type: none"> • Potential types and examples of acceptable formats for expected evidence, • Varied mechanisms to capture needed records, • The importance of certain attributes to consider when capturing artifacts, • Sufficiency criteria for information collected, • Quality assurance and traceability considerations, and • The rationale for why specific information may be material to demonstrate compliance.
Exhibits:	<p>Where applicable, this section may be included to offer supporting examples of commands, job aids or tools, diagrams or process flows, samples of evidence etc. that Registered Entities may choose to adopt, or adapt, for use to support the execution and continuous improvement of compliance implementations.</p>
Operational Controls Samples:	<p>Provides ideas and examples of operational controls (sometime also referred to as management practices) that may be implemented to attain, maintain, and demonstrate compliance as a byproduct of sound security practices and day-to-day operational activities. Offering a perspective on operational controls fosters an opportunity for the industry to engage in dialogue about operational risk management and ongoing continuous improvement and effectiveness through conformance to internal processes and procedures.</p> <p>This field is not intended to contain those internal controls that independently govern a functional area’s conformance to their daily operational management practices and controls. Guidance on building an internal self-assessment and assurance program that samples operational controls and test them for design effectiveness and sufficiency is contained in the Risk Mitigation and Internal Controls section of this SAG.</p> <p>Note: Because each Registered Entity determines the depth, breadth, and compliance margin for internal controls (where the standard is not prescriptive for timing) generic language such as, “At an interval determined by the Registered Entity” or “On a cycle defined by the Registered Entity” has been used. Controls need to be measurable for effective security and compliance performance, and as such, Registered Entities should consider specifying the actual interval or cycle within which each control is executed.</p>
Supporting Analysis	
<p>Where needed, a supplemental narrative of the SME Team’s supporting analysis where the Requirement Language may have dependencies and cause additional analysis of other Standards and Requirements outside of CIP-010-2 Requirement R1 & R2. This is intended to provide a holistic approach to implementation guidance and a series of tools to aid Registered Entities in recognizing and accommodating for those dependencies.</p>	



EVALUATING CIP-010-2, REQUIREMENT R1, PART 1.1. – 1.5.

Analysis Requirement R1. Configuration Change Management

Requirement Language	
<p>R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].</p>	
Evaluation	
<p>Objective:</p>	<p>The objective of Requirement R1 is to cause Registered Entities to document and implement configuration change processes such that personnel executing tasks have a sustainable and repeatable framework to achieve success in meeting the mandatory obligations of each Part within CIP-010-2 Table R1 – Configuration Change Management.</p>
<p>Value Proposition:</p>	<p>Establishing configuration change processes that leverage established baselines allows Registered Entities to identify significant changes to trigger change control, configuration management, and security assessment and testing procedures.</p> <p>Changes that affect attributes of established baselines for any Cyber Asset come with some level of risk. Whether the change is intended to adjust functionality or feature sets, address a security vulnerability, and/or fix an operational performance issue; implementing changes can introduce unexpected/unintended results that could negatively impact operational security controls.</p> <p>Knowing the expected configuration baseline of a Cyber Asset is an important first step in the processes toward assessing and mitigating this risk. Effectively monitoring, managing, and approving changes to established baselines are equally important.</p>
Recommended Application Guidance – Potential Approaches	
<p>To support achievement of compliance at the main requirement level, a process could be characterized as a collection of interrelated tasks intended to solve a particular problem or perform a particular function. Processes typically describe the organizational accountability and sequencing of tasks to accomplish specific actions focusing on the input and output of the action, as well as what data and information flows through the process.</p> <p>Documented Configuration Change Management processes may be used to provide a standardized enterprise or cross-functional framework on what phases are expected to be executed in what order when the process is operating as designed. This may help identify interdepartmental dependencies and/or where systems and human actions intersect. Several industry best practices and frameworks (as referenced in the Methodology section of this SAG) can serve as a guideline to establishing a robust process that also accomplishes the objective and minimum mandatory obligations within CIP-010-2 Requirement R1.</p> <p>Process documents may also be supported by instructional steps detailed at a Standard Operating Procedure (SOP) level, or a Departmental Operating Procedure (DOP) level, depending on the Registered Entity's organizational structure, applicable Cyber Assets/Systems, and operational or technical nuances</p>	



between departments. Processes can be in the form of standalone narrative documents, independent documents that depict a work flow or process diagram, or a combination of narratives and illustrations.

A configuration change management system typically supports the execution of a documented process and may be in the form of 3rd Party Tools like but not limited to an existing work order management system, a standalone database or spreadsheet, or even a custom application. Registered Entities do not have to implement a 3rd Party Tool to accomplish compliance. Other options could be less sophisticated in nature and leverages administrative tools like but not limited to manually populated change control forms, checklists, review and approval routing through intra company mail, or office productivity applications like e-mail or manually populated online forms.

Whichever process(es) or tools your organization implements, ease of use and consistency are key to success. Consideration the following items may serve to help reduce risk and shape or guide the chosen approach toward a solution that is repeatable, sustainable, and works best for your organization:

- Without a change management process an intentional change could unintentionally disrupt reliability if all the potential effects or dependencies of the change are not evaluated.
- A change management program allows changes to be coordinated with other planned systems outages to minimize the outage effect the collective changes may have on the system. Even with redundant systems, a direct outage may not occur but there is risk if a backup system is inoperable and the redundancy negated during a change.
- Consider how the change management process addresses emergency vs. scheduled or routine changes.
- Consider whether the change management process is best managed; centrally or as a distributed process. For instance, control center EMS/SCADA systems may utilize one method to track change and substation systems may use another.

If technology is used, it is recommended that the change management system(s) have the capability to distribute automated reminders to SMEs and track work status to completion to help remove human factors that could impact successful change implementation or timely response to unforeseen outcomes.

Tip:	Consider adding check points in the change management process to check if incident response or disaster recovery plans are affected by a change. This could be CIP-008 or CIP-009 plans, or enterprise plans. For instance, upgrading hardware or backup software may change the method in which a Cyber Asset is recovered.
Lessons Learned:	With the complexity of most IT/OT systems it may be difficult to have an expert on each, and every, system as well as be informed on outage schedules of interdependent systems. Consider establishing a “Change Review Board”. As one approach, this can be a group of Subject Matter Experts (SMEs) that manage the different aspects of the applicable Cyber Assets along with the manager(s)/supervisor(s) that approve the system changes.
Evidence:	<u>Process Records</u> Documented Process(es). Registered Entities should establish and retain copies of the implemented process(es) narrative(s) and/or diagram(s) that collectively include Requirement Parts 1.1 – 1.5. Where process(es) are documented in both narrative form and process flow diagrams, Registered Entities are best served to assure the two align. Some considerations to help assure sufficiency of this evidence includes producing dated process(es) and approval records that capture attributes such as Revision History, Effective



<p>Evidence: (continued)</p>	<p>Date, Approver Name/Role, Approval Signature, and Approval Date. Registered Entities may define the approver as an individual or a committee.</p> <ul style="list-style-type: none"> • Revision History: Demonstrates the life and maturity of the process(es). Helps to demonstrate compliance timeframes for review cycles or necessary updates are met and that a Registered Entity is continuously improving process(es) and maintaining alignment between documented expectations and operational practices. • Effective Date: Demonstrates the expectation for when the process(es) are to be fully implemented and operationalized and provides reasonable assurance that the process(es) were established and available for use on or before the date the Standard Requirement(s) became effective and enforceable. • Approver Name/Role: Helps assure the person(s) approving the process operates in a position with the authority and resources to prioritize work and operationally execute in conformance with the documented configuration change management activities. • Approval Signature: A wet ink signature(s) or a digital approval(s) provides reasonable authentication of the signer and demonstrates that leadership in alignment with the intent, purpose, and activity prescribed by the CIP Requirement(s) and process(es). For sufficiency, the signature should be that of the Approver Name/Role or another employee that serves as that person's/department's leader (i.e. the Manager's Director, or VP etc.) • Approval Date: Demonstrates process(es) were established and approved on or before the date the Standard Requirement(s) became effective and enforceable. For sufficiency, Approval Date should be on or before the Effective Date to demonstrate leadership awareness and agreement with implementation timing. <p><u>Potential Supporting Process Attributes/Content</u></p> <p>Cyber Asset scope, Functional Area Accountability, and Roles and Responsibilities documentation, either within the process(es) or in a referenced document or tool (such as an Accountability Matrix) can help demonstrate the process(es) are communicated and implemented thereby reducing the risk of human performance errors. If this practice is used, this documentation should be dated and retained as compliance evidence with the process(es) records</p> <p><u>Potential Supporting Records</u></p> <ul style="list-style-type: none"> • A Requirement Mapping, either within the process itself or as a separate supporting record, can help provide traceability between the steps or elements of the process(es) and each applicable Requirement Part to help assure collective inclusion of all necessary components in demonstration of compliance with each part. • Process and/or Workflow Diagrams for technologies/tools that govern, automate, or otherwise have a role in the execution of the documented process(es). This type of artifact can illustrate the sophistication of technical internal controls and help to demonstrate repeatability of the process used to comply. • Artifacts from systems can be used in demonstration of implementation of the documented process(es). Manual or <i>system-generated</i> baselines for applicable Cyber Assets demonstrate required information to trigger change is available to facilitate compliance with executing the process(es). Change requests, approvals, security assessments and testing records all show the auditor that process(es) are operationalized.
---	---



Exhibits:	See Exhibit A: Requirement R1., Configuration Change Management (3rd Party Tool Options) for Sample Process Flow Diagrams.
Operational Controls Samples:	<ul style="list-style-type: none"> • Prior to the enforcement date of CIP-010-2 Requirement R1 for applicable Cyber Assets/Systems, the owner(s) of applicable Cyber Assets/Systems establish approved processes that collectively include the establishment of baselines, authorization for deviations from established baselines, maintenance of baseline documentation within 30 calendar days of authorized changes, pre-change security impact assessments, and post-change security posture testing. Processes include provisions for high-impact pre-testing in a non-production environment. • Per occurrence, approved process(es) are communicated to SMEs with a role in configuration change management and published in a repository that provides SMEs access to the process(es). • At a minimum, on a cycle of once per 15 calendar months, or more frequently based on need, the process owner(s), in collaboration with the affected SMEs, performs a review of the documented process(es), updates as needed to align with compliance requirements and operational practices, and executes procedures for re-approval and publication of revised processes to assure organizational alignment and availability of expected practices for SMEs. • At a minimum, on a cycle of once per 15 calendar months¹, or more frequently based on need, and where 3rd Party Tools are used to support the execution of configuration changes processes, the process owner(s) (in collaboration with the affected SMEs) performs a gap analysis between the documented process(es) and the supporting technology to assure alignment between documented expectations and implemented technical controls within supporting 3rd Party Tools. • At a minimum, on a cycle of once per 15 calendar months, or more frequently based on need, the process owner(s) document any identified variances between established processes, operational practices, and/or supporting technology, provides management with recommendations to address variances; establishes, executes, and tracks status of a dated plan to align the documented processes to implemented practices and technology; and informs the compliance team of any potential instances of non-compliance for evaluation and reporting (if needed) to assure controls are effectively designed, operating as intended, and regulatory obligations are met.

¹ While not prescribed by the Standard, the CIP SMET generally recommends Registered Entities consider using an annual, rolling 12-month cycle to leave an extra 3 months to allow scheduling flexibility without compliance issues.



CIP-010-2 REQUIREMENT R1 - CONFIGURATION CHANGE MANAGEMENT

Analysis, Part 1.1. – Developing Baselines

Requirement Language			
CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	High and Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
Evaluation			
Objective:	The objective of Requirement R1 Part 1.1 is to establish the minimum baseline attributes that Registered Entities must identify, document, and manage to assure changes that can potentially affect the security posture of a Cyber Asset trigger change control, configuration management, and security assessment and testing procedures.		
Value Proposition:	<p>Benefits of having established configuration baselines for applicable Cyber Assets, either the individual host level or for a given category of infrastructure, include knowledge and awareness about:</p> <ul style="list-style-type: none"> • Known and expected state • Needed operational settings/parameters • Security design and posture <p>Established, maintained baselines help identify unapproved changes; reducing risk of uncontrolled changes that could lead to instability or inoperability of Cyber Assets that support safe, secure, resilient, and reliable operation of the BES.</p>		



Evaluation (continued)	
Value Proposition: (continued)	<p>Baselines also provide a repeatable foundation to consistently configure applicable² Cyber Assets to align with a preapproved state deemed operationally sound and secure.</p> <p>Baselines inform the Cyber Asset owner how to assess vulnerabilities and mitigate threat/attack vectors further reducing risk.</p> <p>Baselines also provide data to make informed decisions when investigating/recovering from incidents or evaluating security posture of a Cyber Asset. Establishing baselines also serves to partially support CIP-007-6 Requirement R1 & R2 mandatory regulatory obligations.</p>
Tip 1:	<p>Centralizing baseline configuration tracking can help:</p> <ul style="list-style-type: none"> • Provide a holistic view of a Registered Entity’s install base, thereby assisting the Registered Entity in lifecycle management of Cyber Assets and associated software. • Standardize by identifying where one-off solutions may be implemented, or where dependencies on legacy or end-of life hardware or software exist.
Lessons Learned:	<p>Some Cyber Assets may not support, or be technically capable, of using one of the five defined baseline attributes. For SMEs with intimate knowledge of these Cyber Assets, it may seem intuitive to leave the attribute blank. Blank attributes leave it unclear if the attribute was considered and intentionally blank, or if the attribute tracking was missed. To demonstrate compliance, consider standardizing the approach to handling how to document such attributes to prevent assumptions and so the auditor can draw the same conclusion as the SME based on evidence such as vendor manuals or release notes that detail the technical preclusions.</p>
Evidence:	<p>Established baselines could be a single document or export from a system that tracks all five attributes or a set of records from multiple data sources that collectively includes all five attributes. Baseline documentation can also be at the individual Cyber Asset level, or in groupings of Cyber Assets with commonality that have the same baseline. Evidence should uniquely identify each Cyber Asset and provide traceability to each attribute. Where groupings are used, the documentation should provide enough detail to trace back to the population of uniquely identified Cyber Assets in that group. Baselines should include the established date. Consider assigning an approver to sign and date the records on or before the effective date of the baseline to demonstrate leadership engagement in the process and agreement that the configuration constitutes the approved expected state.</p>
Operational Controls Samples:	<p>Upon the first application of the BES Cyber System assessment methodology pursuant to CIP-002-5.1a Requirement R1, populations of identified Cyber Assets are evaluated against a checklist of baseline requirements, and baselines are established and approved upon commissioning and prior to the effective date relative to the BES Cyber System.</p>

² The use of the term applicable refers to the Cyber Asset listings within the Applicable Systems column of each Requirement Part of each Table relevant to CIP-010-2 Requirements R1 & R2.



Evaluation (continued)**Operational Controls Samples:**
Continued

At a minimum, on a cycle of once per 15 calendar months, as a part of active vulnerability assessments pursuant to CIP-010-2 Requirement R3, populations of Cyber Assets are evaluated against a checklist of baseline requirements, and baselines are verified to assure compliance is maintained and re-approved as a detective control to CIP-010-2 Requirement R1 Part 1.3.

As a part of the change control process, prior to implementing a new or replacement Cyber Asset into production, compare new device configurations to the established baseline for a similar Cyber Asset type or group to assure it is configured as expected.

Prior to procurement, and as a part of the supply chain process, new hardware and/or software solutions are evaluated against a checklist of baseline requirements to assure the Cyber Asset(s) can meet the security requirements and mandatory obligations for CIP.

Recommended Application Guidance – Potential Approaches**3rd Party Tool Options**

While it is difficult to find a tool that accomplishes 100% of the tasks, tools can help automate some tasks. This application guide cannot provide vendor names³ but discusses areas to consider for implementing a tool.

There are two potential approaches when implementing tool-based solutions: agents or agentless (native vs non-native). When determining which approach to employ, Registered Entities have several things to consider including but not limited to the category of infrastructure, the level of capabilities needed, support contract terms, and/or cost considerations.

These tools often use an agent to gather the information from the system.

- An agent is a small software package installed on the local system to report back local system data to the management console.
- Agentless 3rd Party Tools directly query systems without locally installed software. This feature can be valuable for gathering information from firmware-based equipment such as network switches, routers, firewalls, IP to serial converters and other console only based devices unable to support an agent. This can also be useful if a vendor or 3rd party support does not recommend installing an agent.

The same tool can be utilized in different ways.

- The tool can be strictly used for its native function to gather data, or
- The tool can be integrated with in-house written application(s) to consume, process, and store the data

³ NERC application guides are vendor agnostic, so the names of the tools utilized by the authors of this guide cannot be provided. However, these third-party tools are some of the same tools you will find being utilized for normal business IT management functions like system inventory, vulnerability management, file integrity monitoring and security configuration management. Several members of the MRO CIP SME team have implemented such tools.



Recommended Application Guidance – Potential Approaches (continued)

3rd Party Tool Options (continued)

One benefit of using a 3rd Party Tool to gather the data is it typically provides data integrity aspects such as encryption and hashing. A 3rd Party Tool's strength lies in its ability to quickly gather *system-generated* data and perform comparisons to previously gathered data. Tools like this also typically contain features to generate alarms or send alerts when variances are discovered. The ability to automate comparing the current state to expected, approved states can serve as a detective control supporting cybersecurity and compliance objectives.

Tip 1:	The system may also meet CIP-010-2 Requirement R2 elements. Leveraging the financial investment to accomplish multiple requirements supports cost prudence. Having an automated system to meet this requirement can save hours of labor and improve accuracy.
Tip 2:	Also consider contacting the EMS/SCADA vendor prior to implementing a 3rd party solution to verify they support it.
Tip 3:	Place good security around the management console because it typically has administrative access to all systems. If it were compromised, an attacker would have the “keys to the kingdom.”
Tip 4:	A test environment is recommended. Having a separate system configured like the production system in a test environment allows testing of new versions, agents, and configurations prior to implementing in production.
Tip 5:	As a general practice, Registered Entities may want to generate and retain a point in time snapshot of the baseline upon the completion of changes as evidence that updates occurred within compliance timeframes.
Lessons Learned 1:	These tools take planning, testing, and understanding of internal systems to be successfully implemented.
Lessons Learned 2:	Registered Entities should consider the human resources a 3rd Party Tool requires to implement and maintain. MRO CIP SME team members found implementing a 3rd Party Tool took significant manpower, but once implemented, the tool quickly and accurately gathered system baselines.
Lessons Learned 3:	If leveraging external expertise, consider how knowledge transfer will occur and/or what external support contracts may be needed to assure skilled resources are available to properly maintain and tune the system over time.
Lessons Learned 4:	A 3rd Party Tool(s) is likely to become a primary source of records to demonstrate compliance, configuring an accurate and reliable time source (whether local, ntp server, or gps clock etc.) becomes necessary.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Lessons Learned 5:	The 3rd party system may be subject to other CIP requirements depending on where the system logically resides and the functions it performs.
Evidence:	<p>Evidence should clearly trace to the five required baseline attributes and include uniquely identifiable information about the Cyber Asset to provide traceability to the pertinent equipment. If grouping Cyber Assets, assure documentation clearly identifies which Cyber Assets are represented by the baseline grouping.</p> <p>Where system fieldnames vary from the required baseline attributes, Registered Entities should consider documenting a mapping between the fields in the 3rd Party Tool and the requirements to provide ultimate clarity for evidentiary records generated from the system. Where reports are run on demand, assure evidence is dated and timestamped by the system, clearly reflects all relevant attributes, and identifies the Cyber Asset(s) or groupings that are pertinent. If relying on a 3rd Party Tool to house baseline configuration information as the authoritative source for query of on demand records, assure the system is backed up and that backup are tested so records required to demonstrate compliance with timeframes for establishing and updating baselines are available during audit. If relying on a 3rd Party Tool, leverage inherent audit logging features to assure the authenticity and integrity of records and historical changes.</p>
Operational Controls Samples:	<ol style="list-style-type: none"> 1. Establishment and approval of configuration baselines is an item on the Cyber Asset commissioning checklist. 2. Automated tools are configured to interrogate regulated subnets on a scheduled basis and capture discoverable baseline attribute data for newly connected routable Cyber Assets. 3. On cycle of once per quarter the compliance team samples 10% of Change Control records for the addition of newly commissioned Cyber Assets and tests to assure baselines were established and approved pursuant to the Functional Area Checklist.
Manual Options	
<p>Manual processes can be time and manpower intensive but are often necessary in generation and transmission environments. They can also be useful in immature programs because they are easily adaptable. A structured approach to change and continuous improvement may increase the speed of changes and reduce time and manpower requirements. The OODA (Observe, Orient, Decide, Act) loop is one structured approach to consider for evaluating manual processes. OODA loops consist of observing the situation, orienting or processing the situation, deciding on a solution, and acting on the solution. This loop continues to cycle until achieving the desired change management process.</p> <p>Using a manual approach is one option for baselining configurations of applicable Cyber Assets that:</p> <ol style="list-style-type: none"> 1. Are not networked using a routable protocol or 2. Have Local Area Network connectivity within an isolated Electronic Security Perimeter (ESP) without an Electronic Access Point (EAP). 	



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
<p>For operating system-based devices (i.e. Microsoft Windows and Linux based devices such as HMIs), running custom batch scripts locally can capture baseline configuration to text files.</p> <p>For firmware-based devices, such as protective relays, the local LCD display’s information can be manually recorded. Firmware based device baseline configuration can typically be obtained by connecting directly to the device using a terminal program or vendor software, navigating through menus, or through executing specific commands, and ‘capturing’, exporting, or otherwise saving the information to a file(s).</p> <p>Using a spreadsheet or database to collect baseline information is one method for initially collecting and storing the required baseline attributes. Spreadsheets may be quicker to create and easily edit, and databases may take more time to create but might be easier to update and search. Standardizing devices, firmware, and configurations for BCAs and BCSs reduces workload and makes it easier to spot unauthorized changes. Manually baselining BCAs and BCSs forces the SMEs to become familiar with expected device settings.</p>	
Tip:	As a general practice, Registered Entities may want to generate and retain a point in time snapshot of the baseline upon the completion of changes as evidence that updates occurred within compliance timeframes.
Lessons Learned:	Manually collecting Cyber Asset attribute information needed to establish baselines may require connecting a Transient Cyber Asset or Removable Media, and Registered Entities may want to consider documented steps or controls associated to mandatory obligations of CIP-010-2 Requirement R4 as a reminder to SMEs performing the baselining activity. As examples, a procedure, checklist, or physical mechanisms like port blockers, tamper tape, or signage could serve as reminders.
Evidence:	The resulting text files or manually recorded attribute data can be stored as the baseline documentation. This information could be stored with the device in an existing asset management system, or in an organized file structure or document management system. For simple baseline configuration, such as firmware version, the baseline configuration could be manually entered as an attribute for a device in an asset management system. Consider utilizing a system that has version control as it is important to retain version history as compliance evidence.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. Upon commissioning, a Cyber Asset commissioning checklist containing all five required attributes is used to manually collect actual configuration and establish baselines. 2. On a cycle pre-defined by the Registered Entity, a Change Advisory Board (CAB) reviews completed changes for additions of applicable Cyber Assets and verifies individual configuration baselines have been established, or Cyber Assets are part of a grouping with a pre-established standardized baseline. Note: a cycle of once per month could also serve as a preventative control for CIP-010-2 Requirement R1.3. 3. On a cycle pre-defined by the Registered Entity, the compliance team samples 10% of Change Control records for the addition of newly commissioned Cyber Assets and performs self-assessment testing to assure baselines were established and approved pursuant to the functional area checklist.



CIP-010-2, REQUIREMENT R1, PART 1.1 – DEVELOPING BASELINES

Analysis, Part 1.1.1. – Operating System or Firmware Versions

Requirement Language (intentionally abbreviated to Part 1.1.1.)		
CIP-010-2 Table R1 – Configuration Change Management		
Part	Applicable Systems	Requirements
1.1	High and Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Develop a baseline configuration, individually or by group, which shall include the following item: <ol style="list-style-type: none"> 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
Evaluation		
Objective:	The objective of Requirement R1 Part 1.1.1. is to identify and document the installed version of any Operating System (OS) or Firmware (FW) in use on applicable ⁴ Cyber Assets to assure: <ul style="list-style-type: none"> • Effective inventory, lifecycle, vulnerability, and risk management of OS/FW versions • During normal operations: <ul style="list-style-type: none"> ○ The expected state of OS/FW and version is clearly understood for personnel responsible for implementing, supporting, and maintaining the implemented OS/FW, ○ Changes or upgrades to OS/FW versions trigger change control processes and authorizations, and ○ Configuration management and monitoring processes are inclusive of running, installed OS/FW versions, and designed to detect unauthorized changes 	
Value Proposition:	There are several benefits to tracking OS/FW version that collectively provide compliance, security, and reliability value. Documenting the approved and expected versions of OS/FW tracks the initial state of installation, and has the following additional benefits: <ol style="list-style-type: none"> 1. Effective management of documentation that tracks OS/FW version serves to partially support mandatory regulatory obligations to comply with CIP-007-6 Requirement R2. By recognizing this synergy, Registered Entities can realize efficiency gains by leveraging one process or tool to accomplishing both compliance obligations. OS/FW version tracking supports CIP-007-6 Requirement R2 compliance activities and security objectives when used to identify and document patch sources, ascertain applicability, to streamline review/assessment of patch releases in scope for the Registered Entity, and making informed decisions to mitigate vulnerabilities. 	

⁴ The use of the term applicable refers to the Cyber Asset listings within the Applicable Systems column of each Requirement Part of each Table relevant to CIP-010-2 Requirements R1 & R2.



Evaluation (continued)	
<p>Value Proposition: (continued)</p>	<ol style="list-style-type: none"> 2. Similarly, the benefit of documented OS/FW versions is not just maintaining compliance; it also provides the added business value of supporting reviews of imminent or released upgrades, fixes, and feature enhancements that may improve operational stability or capability of the system. 3. Effectively managing OS/FW version tracking documentation also serves to position Registered Entities for successful performance of the remaining mandatory regulatory obligations to comply with CIP-010-2 Requirement R1 Parts 1.2 – 1.5 by helping to assure: <ul style="list-style-type: none"> ○ Prior to the implementation of OS/FW version changes <ul style="list-style-type: none"> ● Authorization and documentation for OS/FW baseline changes is completed pursuant to Requirement R1 Part 1.2, ● Security control impact assessments are evoked pursuant to Requirement R1 Part 1.4, and ● Controlled functionality testing procedures are executed for applicable high impact Cyber Assets/Systems pursuant to Requirement R1 Part 1.5 ○ Following the implementation of OS/FW version changes <ul style="list-style-type: none"> ● Post-change security controls testing procedures are evoked pursuant to Requirement R1 Part 1.4, and ● Established baselines are brought up-to-date to reflect actual running, installed versions of OS/FW pursuant to Requirement R1 Part 1.3 4. Effectively managing OS/FW version tracking documentation also serves to partially support mandatory regulatory obligations to comply with CIP-010-2 Requirement R2 for applicable high impact Cyber Assets/ Systems. Documenting what OS/FW versions should be installed supports processes and controls to detect, identify, respond, and/or recover from unintentional or unapproved changes, thereby reducing the volume of uncontrolled changes and minimizing the risk of causing instability or inoperability of Cyber Assets needed to support safe, secure, resilient, and reliable operation of the BES.
Recommended Application Guidance – Deep Dive into Part 1.1.1.	
3rd Party Tool Options	
<p>3rd Party Tools can help Registered Entities to achieve and maintain compliance with Requirement R1 Part 1.1.1. Many tools can gather the operating system version of common platforms like, but not limited to, Microsoft Windows, Linux and UNIX variants, Cisco IOS etc. However, some 3rd Party Tools do not provide agents for all variants of the operating system nor support certain legacy operating systems or discovery and collection of firmware and version. Some tools support console connections to a client and can run commands remotely to retrieve the operating system or firmware version information.</p>	
Tip:	<p>Checking with the vendor prior to purchasing a product helps avoid being locked into to using older versions of the software.</p>



Recommended Application Guidance – Deep Dive into Part 1.1.1. (continued)	
3rd Party Tool Options (continued)	
Lessons Learned 1:	<p>Registered Entities are not expected to track things that are not explicitly included in CIP-010-2 Requirement R1 Part 1.1.1; however, Registered Entities may choose to add other attributes to established baselines and/or leverage other programs used comply with CIP to achieve CIP-010-2 baselines. While it may not be immediately obvious when discussing the OS/FW attribute, this could catch OS based devices that also have firmware and prevent a potential gap in identified security patch sources to support CIP-007-6 R2.</p> <p>As the CIP Standard evolved, nuances between the language for the security patching requirement of CIP-007-3 R3 and CIP-007-6 R2 were introduced, and this may cause unintended consequences in BIOS (Basic Input/Output System) -level software updates that may affect the 1.1.5 baseline attribute, particularly if a BIOS-level security patches is identified pursuant to CIP-007-6 R2.1 for cyber security patches. The wording of the CIP-007-6 standard changed from version 3 to version 6; version 3 used to qualify security patches with the word “software” whereas version 6 has this word removed. Including hardware-based security patch sources in this program creates a defensible position for this nuance.</p> <p>Consider the situation where a Microsoft Windows or Linux based computer system (workstation or server) BIOS has been issued a security update. If this firmware was not previously tracked as part of requirement 1.1.1 it should be tracked as part of 1.1.5 if the security update is applied. Identifying, tracking, evaluating, and installing cyber security patches for applicable Cyber Assets is a requirement of CIP-007-6.</p>
Evidence:	<p>Recommended evidence to retain could be, and is not limited to, reports, exports, or in-system database records or logs of the OS/FW version. Assure the evidence captured is sufficient to demonstrate compliance.</p> <p>Consider including the following attributes in the records retained to demonstrate compliance, as well as quality control mechanisms to help assure material information is present, legible, and not truncated:</p> <ul style="list-style-type: none"> • Date/Time demonstrating when 3rd Party Tools outputs were generated, whether within the in-system log or exported as separate evidentiary artifact • Date/Time demonstrating when each baseline was established/approved • Unique ID ⁵ of each applicable Cyber Asset for traceability to the baseline and assurance the full population is covered.

⁵ Registered Entities should consider determining what attribute(s) of High and Medium impact BES Cyber Systems/Assets and associated Applicable Systems is to be used as a unique ID. An ability to uniquely identify each Cyber Asset provides traceability between the population, activities performed, and supporting records to demonstrate compliance.



Recommended Application Guidance – Deep Dive into Part 1.1.1. (continued)	
3rd Party Tool Options (continued)	
Exhibits:	See Exhibit C: Part 1.1.1. – Operating System or Firmware Versions (3rd Party Options) for a sample <i>system-generated</i> report:
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. During the software evaluation processes, trial versions of 3rd Party Tools are tested for the ability to gather evidence for Part 1.1.1 to assure procured products meet mandatory regulatory obligations
Manual Options	
<p>The operating system version on Microsoft Windows and Linux devices can be captured to a text file using commands in a batch script. If available, using a Graphical User Interface (GUI), like the Windows Control Panel as an example, can be another option to retrieve and document the operating system version.</p> <p>Firmware version for firmware-based devices can typically be captured to a text file by connecting locally to the device and running commands in a terminal connection or saving output from vendor software. Depending on the device capabilities, navigating through the menu on a device’s local LCD display and manually recording the observed version can obtain the operating system version.</p>	
Tip:	Storing the firmware version history with the device in an existing asset management or protection system settings program prevents having to maintain device information in multiple locations.
Lessons Learned 1:	<p>Registered Entities are not expected to track things that are not explicitly included in CIP-010-2 Requirement R1 Part 1.1.1; however, Registered Entities may choose to add other attributes to established baselines and/or leverage other programs used comply with CIP to achieve CIP-010-2 baselines. While it may not be immediately obvious when discussing the OS/FW attribute, this could catch OS based devices that also have firmware and prevent a potential gap in identified security patch sources to support CIP-007-6 R2.</p> <p>As the CIP Standard evolved, nuances between the language for the security patching requirement of CIP-007-3 R3 and CIP-007-6 R2 were introduced, and this may cause unintended consequences in BIOS-level software updates that may affect the 1.1.5 baseline attribute, particularly if a BIOS-level security patch is identified pursuant to CIP-007-6 R2.1 for cyber security patches. The wording of the CIP-007-6 standard changed from version 3 to version 6; version 3 used to qualify security patches with the word “software” whereas version 6 has this word removed. Including hardware-based security patch sources in this program creates a defensible position for this nuance.</p>



Recommended Application Guidance – Deep Dive into Part 1.1.1. (continued)	
Manual Options (continued)	
Lessons Learned 1: (Continued)	Consider the situation where a Microsoft Windows or Linux based computer system (workstation or server) BIOS has been issued a security update. If this firmware was not previously tracked as part of requirement 1.1.1 it should be tracked as part of 1.1.5 if the security update is applied. Identifying, tracking, evaluating, and installing cyber security patches for applicable Cyber Assets is a requirement of CIP-007-6.
Evidence:	Recommended evidence to retain could be, and is not limited to, the text file outputs from the commands that were executed or screenshots of the OS/FW version. Assure the evidence captured is sufficient to demonstrate compliance. Material attributes to consider including are date information to demonstrate when it was established, the unique ID ⁶ of the Cyber Asset, and a check to assure that material information is not truncated.
Exhibits:	See Exhibit D: Part 1.1.1. – Operating System or Firmware Versions (Manual Options) for a sample script:
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. Documented processes include steps to assure operating system and firmware version are inventoried and documented as part of the baseline. 3. Confirmation of the operating system and firmware version occurs during the periodic scheduled vulnerability assessment pursuant to CIP-010-2 R3 to assure implemented versions align with the approved and expected version.

⁶ Registered Entities should consider determining what attribute(s) of High and Medium impact BES Cyber Systems/Assets and associated Applicable Systems is to be used as a unique ID. An ability to uniquely identify each Cyber Asset provides traceability between the population, activities performed, and supporting records to demonstrate compliance.



CIP-010-2, REQUIREMENT R1, PART 1.1. – DEVELOPING BASELINES

Analysis, Part 1.1.2. – Installed Commercial or Open-source Software

Requirement Language (intentionally abbreviated to Part 1.1.2.)		
CIP-010-2 Table R1 – Configuration Change Management		
Part	Applicable Systems	Requirements
1.1	High and Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Develop a baseline configuration, individually or by group, which shall include the following item: <ol style="list-style-type: none"> 1.1.2. Any commercially available or open-source application software (including version) intentionally installed
Evaluation		
Objective:	The objective of Requirement R1 Part 1.1.2. is to identify and document the name and version of application software ⁷ (commercially available or open source) that is intentionally installed on applicable Cyber Assets to assure: <ul style="list-style-type: none"> • Effective inventory, lifecycle, vulnerability, and risk management of application software and versions • During normal operations: <ul style="list-style-type: none"> ○ The expected state of application software and version is clearly understood for personnel responsible for implementing, supporting, and maintaining the implemented application software, ○ Changes or upgrades to application software versions trigger change control processes and authorizations, and ○ Configuration management and monitoring processes are inclusive of running, installed application software versions, and designed to detect unauthorized changes 	
Value Proposition:	There are several benefits to tracking application software versions that collectively provide compliance, security, and reliability value. Documenting the approved and expected versions of application software tracks the initial state of installation, and has the following additional benefits:	

⁷ The use of the term application software in this section refers to those commercially available or open-source applications that the Registered Entity has chosen to intentionally install on Cyber Assets subject to the listed Applicable Systems in CIP-010-2 Table R1 – Configuration Change Management, Requirement R1, Part 1.1.2.



Evaluation (continued)**Value Proposition:**

(continued)

1. Effective management of documentation that tracks application software version serves to partially support mandatory regulatory obligations to comply with CIP-007-6 Requirement R2. By recognizing this synergy, registered entities can realize efficiency gains by leveraging one process or tool to accomplishing both compliance obligations. Application software version tracking supports CIP-007-6 Requirement R2 compliance activities and security objectives when used to identify and document patch sources, ascertain applicability to streamline review/assessment of patch releases in scope for the Registered Entity, and making informed decisions to mitigate vulnerabilities.
2. Similarly, the benefit of documented application software versions is not just maintaining compliance; it also provides the added business value of supporting reviews of imminent or released upgrades, fixes, and feature enhancements that may improve operational stability or capability of the system.
3. Effectively managing application software version tracking documentation also serves to position Registered Entities for successful performance of the remaining mandatory regulatory obligations to comply with CIP-010-2 Requirement R1 Parts 1.2 – 1.5 by helping to assure:
 - Prior to the implementation of application software version changes
 - Authorization and documentation for application software baseline changes is completed pursuant to Requirement R1 Part 1.2,
 - Security control impact assessments are evoked pursuant to Requirement R1 Part 1.4, and
 - Controlled functionality testing procedures are executed for applicable high impact Cyber Assets/Systems pursuant to Requirement R1 Part 1.5
 - Following the implementation of application software version changes
 - Post-change security controls testing procedures are evoked pursuant to Requirement R1 Part 1.4, and
 - Established baselines are brought up-to-date to reflect actual running, installed versions of application software pursuant to Requirement R1 Part 1.3
4. Effectively managing application software version tracking documentation also serves to partially support mandatory regulatory obligations to comply with CIP-010-2 Requirement R2 for applicable high impact Cyber Assets/Systems. Documenting what application software versions should be installed supports processes and controls to detect, identify, respond, and/or recover from unintentional or unapproved changes, thereby reducing the volume of uncontrolled changes and minimizing the risk of causing instability or inoperability of Cyber Assets needed to support safe, secure, resilient, and reliable operation of the BES.



Recommended Application Guidance – Deep Dive into Part 1.1.2.

3rd Party Tool Options

3rd Party Tools can identify software programs residing on operating system based Cyber Assets. Tools can be used to inventory executables and libraries. With this capability comes a downside, the tools typically identify all executables and libraries including the ones associated with the operating system. The tools provide some methods of excluding areas to search for programs “tuning” the system. In many cases, it is better to allow the program to inventory everything because it provides a documented baseline able to identify changes when a patch is applied to underlying programs of an operating system.

Firmware-based Cyber Assets do not typically support the installation of commercially available or open-source software, therefore this attribute may not be applicable to those types of devices. Registered Entities may choose to define and record an affirmative value to indicate this condition, such as ‘N/A’, ‘not applicable’, ‘none’, ‘firmware-based only’, etc. as opposed to a null or blank field in a manually maintained baseline. Programmatically defining how this attribute is documented helps assure clarity that the attribute was evaluated and understood to be irrelevant and can prevent confusion or the misperception of an incomplete baseline.

Tip:	For Firmware-based Cyber Assets, if there is no commercially available or open-source application software (including version), established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.
Lessons Learned:	Registered Entities should consider opening a dialogue with vendors to gain a thorough understanding of how commercial software is registered and any path(s) used to house executables and/or libraries to help assure monitoring exclusions do not hinder a Registered Entity’s ability to meet baseline configuration change, update, and monitoring requirements and compliance timeframes.
Evidence:	<p>Recommended evidence to retain could be, and is not limited to, reports, exports, or in-system database records or logs of the commercially available or open-source software and version. Assure the evidence captured is sufficient to demonstrate compliance.</p> <p>Consider including the following attributes in the records retained to demonstrate compliance, as well as quality control mechanisms to help assure material information is present, legible, and not truncated:</p> <ul style="list-style-type: none"> • Date/Time demonstrating when 3rd Party Tools outputs were generated, whether within the in-system log or exported as separate evidentiary artifact • Date/Time demonstrating when each baseline was established/approved • Unique ID of each applicable Cyber Asset for traceability to the baseline and assurance the full population is covered



Recommended Application Guidance – Deep Dive into Part 1.1.2. (continued)	
3rd Party Tool Options (continued)	
Exhibits:	See Exhibit E: Part 1.1.2. & 1.1.3. – Installed Commercial, Open-source, or Custom Software (3rd Party Tool Options) for an example of a <i>system-generated</i> report.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. During the software evaluation processes, trial versions of 3rd Party Tools are tested for the ability to gather evidence for Part 1.1.2 to assure procured products meet mandatory regulatory obligations.
Manual Options	
<p>Batch scripts can capture commercially available or open-source application software versions on Microsoft Windows and Linux devices to a text file. Another approach is to use native, local utilities that inventory the installed software and manually recording the observed output. If relying on an output of the Operating System's registry, Registered Entities may want to employ a process to validate expected software properly registers. One approach to validate the commercially available or open-source application software registration is to compare a walk down of directories to the registry output.</p> <p>Firmware-based Cyber Assets do not typically support the installation of commercially available or open-source software, therefore this attribute may not be applicable to those types of devices. Registered Entities may choose to define and record an affirmative value to indicate this condition, such as 'N/A', 'not applicable', 'none', 'firmware-based only', etc. as opposed to a null or blank field in a manually maintained baseline. Programmatically defining how this attribute is documented helps assure clarity that the attribute was evaluated and understood to be irrelevant and can prevent confusion or the misperception of an incomplete baseline.</p>	
Tip:	For Firmware-based Cyber Assets, if there is no commercially available or open-source application software (including version), established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.
Lessons Learned:	If using batch scripts to capture software versions, ensure scripts capture each installed software's version number because software version information can be stored in various locations.
Evidence:	Recommended evidence to retain could be, and is not limited to, the text file outputs from the commands that were executed or screenshots from a directory or locally installed utility of the commercially available or open-source application software. Assure the evidence captured is sufficient to demonstrate compliance. Material attributes to consider including are date information to demonstrate when it was established, the unique ID of the Cyber Asset, and a check to assure that material information is not truncated.
Exhibits:	See Exhibit F: Part 1.1.2. & 1.1.3 – Installed Commercial or Open-source Software (Manual Options) for a sample batch script to 'Export Installed Programs'
Operational Controls Samples:	See Operational Controls Samples for 3rd Party Tools under 1.1.



CIP-010-2, REQUIREMENT R1, PART 1.1. – DEVELOPING BASELINES

Analysis, Part 1.1.3. – Installed Custom Software

Requirement Language (intentionally abbreviated to Part 1.1.3.)		
CIP-010-2 Table R1 – Configuration Change Management		
Part	Applicable Systems	Requirements
1.1	High and Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Develop a baseline configuration, individually or by group, which shall include the following item: <ol style="list-style-type: none"> 1.1.3. Any custom software installed;
Evaluation		
Objective:	<p>The objective of Requirement R1 Part 1.1.3. is to identify and document any custom software⁸ that is intentionally installed on applicable Cyber Assets to assure:</p> <ul style="list-style-type: none"> • Effective inventory, lifecycle, vulnerability, and risk management of custom software and versions • During normal operations: <ul style="list-style-type: none"> ○ The presence of and expected state for custom software is clearly understood for personnel responsible for developing, implementing, supporting, and maintaining the custom software, ○ Changes or upgrades to custom software trigger change control processes and authorizations, and ○ Configuration management and monitoring processes are inclusive of running, installed custom software, and designed to detect unauthorized changes. 	
Value Proposition:	<p>There are several benefits to tracking custom software that collectively provide compliance, security, and reliability value. Documenting the approved and expected custom software tracks the initial state of installation, and has the following additional benefits:</p> <ul style="list-style-type: none"> • Effective management of documentation that tracks custom software serves to provide awareness of the presence of executable code and the operational need for it within a protected critical environment. Knowledge of the need for custom software and tracking changes helps assure Registered Entities have an intimate understanding of critical systems and are able to make informed decisions to control the use and proliferation of custom software and the risk or vulnerabilities it may present to reliable operations. 	

⁸ The CIP SMET offers a perspective in this SAG for 'custom software' relative to differences between software configuration vs customization of open source or commercial software, particularly in the context of applications that use vendor-provided scripts. Due to the many vendors and their unique approaches to application software and design; where clarity is sought, each Registered Entity is encouraged to consult with their regional CEA(s), and/or leverage any documented Technical Rationale from the NERC SDT, NERC CMEP Practice Guides, NERC approved Implementation Guidance, or NERC Lessons Learned.



Evaluation Continued

Value Proposition:

(continued)

- Similarly, the benefit of documented custom software versions is not just maintaining compliance; it also provides the added business value of supporting of unique or emergent business/operational needs that commercially available or open-source software cannot solve, can deliver efficiency and consistency to repetitive or administratively burdensome tasks through automation, can provide a more user friendly experience for personnel that must operate the system, and may be able to offer fixes, or feature enhancements that can improve operational stability or capability of the system.
- Effectively managing custom software tracking documentation also serves to position Registered Entities for successful performance of the remaining mandatory regulatory obligations to comply with CIP-010-2 Requirement R1 Parts 1.2 – 1.5 by helping to assure:
 - Prior to the implementation of custom software changes
 - Authorization and documentation for custom software changes is completed pursuant to Requirement R1 Part 1.2,
 - Security control impact assessments are evoked pursuant to Requirement R1 Part 1.4, and
 - Controlled functionality testing procedures are executed for applicable high impact Cyber Assets/Systems pursuant to Requirement R1 Part 1.5
 - Following the implementation of custom software changes
 - Post-change security controls testing procedures are evoked pursuant to Requirement R1 Part 1.4, and
 - Established baselines are brought up-to-date to reflect actual running, installed custom software pursuant to Requirement R1 Part 1.3
- Effectively managing documentation to track custom software also serves to partially support mandatory regulatory obligations to comply with CIP-010-2 Requirement R2 for applicable high impact Cyber Assets/ Systems. Documenting what custom software versions should be installed supports processes and controls to detect, identify, respond, and/or recover from unintentional or unapproved changes, thereby reducing the volume of uncontrolled changes and minimizing the risk of causing instability or inoperability of Cyber Assets needed to support safe, secure, resilient, and reliable operation of the BES.
- Understanding where custom software is required to support effective and reliable operations may help Registered Entities identify and maintain a skilled resource base commensurate with the application development needs of the Registered Entity. Proprietary knowledge poses risk to any organization and a well maintained custom software inventory may aid an organization in building bench strength and performing appropriate succession planning to mitigate the operational risk that limited or changing staff resources may cause.



Recommended Application Guidance – Deep Dive into Part 1.1.3.**3rd Party Tool Options**

A 3rd Party Tool can assist with inventorying custom installed software. According to the Guidelines and Technical Basis, this requirement includes scripts. 3rd Party Tools may have difficulty identifying scripts because scripts lack a standardized format. For Microsoft Windows operating systems, scripts can be registered in the “Add Remove Programs” or “Programs and Features” portion of the control panel. Refer to the sample script “CurrPorts.reg.txt” provided with this application guide. Registering the scripts allows 3rd Party Tools to easily inventory them. Running the registration script is a manual process, so anytime a script is modified it needs to be registered. Registered Entities may consider implementing Standard Operating Procedures (SOPs) designating locations to store custom scripts or compiled executables, so the tool can be configured to monitor these locations for knowns and unknowns.

Firmware-based Cyber Assets do not typically support the installation of custom software; therefore, this attribute may not be applicable to those types of devices. Registered Entities may choose to define and record an affirmative value to indicate this condition, such as ‘N/A’, ‘not applicable’, ‘none’, ‘firmware-based only’, etc. as opposed to a null or blank field in a manually maintained baseline. Programmatically defining how this attribute is documented helps assure clarity that the attribute was evaluated and understood to be irrelevant and can prevent confusion or the misperception of an incomplete baseline.

Tip 1:	For Firmware-based Cyber Assets, if there is no custom software (including version), established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.
Tip 2:	Depending on how custom software is installed, it may not register the installation attributes properly with the operating system. Some custom software may be copied to the Cyber Asset and therefore not registered with the operating system. Using a custom script to register the custom software installation attributes may be an option. Refer to the sample script “CurrPorts.reg.txt” provided with the Exhibit for this section of this application guide.
Lessons Learned 1:	Registered Entities should consider establishing standardized practices for development, registration, and path used to house custom software, programming code, and/or scripts to help assure monitoring practices include custom software. This can help prevent oversights that may place Registered Entities at odds with baseline configuration change and update requirements and compliance timeframes. It can also assure the Registered Entity can monitor for and detect unauthorized changes to maintain compliance with CIP-010-2 Requirement R2 Part 2.1.
Lessons Learned 2:	Given that the custom software may be located in multiple folders with multiple files that are identified as part of custom software, a documented listing of custom software locations and file names can prevent unauthorized changes from happening.



Recommended Application Guidance – Deep Dive into Part 1.1.3. (continued)**3rd Party Tool Options (continued)**

Lessons Learned 3	<p>Some large software installations, such as an EMS or PACS system, may contain numerous script files as part of the overall software package.</p> <p>Registered Entities should consider how modifications to a script, DLL, or exe file that changes the way in which it executes could make the installation different from the standard vendor installation and track the file(s) that deviate from the system the vendor supplied as a part of the custom software baseline.</p>
Evidence:	<p>Recommended evidence to retain could be, and is not limited to, reports, exports, or in-system database records or logs of the custom software. Assure the evidence captured is sufficient to demonstrate compliance.</p> <p>Consider including the following attributes in the records retained to demonstrate compliance, as well as quality control mechanisms to help assure material information is present, legible, and not truncated:</p> <ul style="list-style-type: none"> • Date/Time demonstrating when 3rd Party Tools outputs were generated, whether within the in-system log or exported as separate evidentiary artifact • Date/Time demonstrating when each baseline was established/approved <p>Unique ID of each applicable Cyber Asset for traceability to the baseline and assurance the full population is covered</p>
Exhibits:	<p>See Exhibit E: Part 1.1.2. & 1.1.3. – Installed Commercial, Open-source, or Custom Software (3rd Party Tool Options) for an example of a <i>system-generated</i> report as well as the sample script named CurrPorts.reg.txt.</p>
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. During the software evaluation processes, trial versions of 3rd Party Tools are tested for the ability to gather evidence for Part 1.1.3 to assure procured products meet mandatory regulatory obligations.

Manual Options

Batch scripts can capture custom software installed on Microsoft Windows and Linux devices to a text file. For another approach, implement a process requiring custom software to be registered on the device during installation, for example through Add/Remove program on Windows. A custom application may not automatically register itself with the Operating System, so Registered Entities should develop a methodology to validate if custom software did register itself and perform an inventory of installed software and determine what constitutes custom as opposed to commercially available. Entities may want to consider applications, software, executable code that can be run independently or called upon by another program (i.e. custom DLL), and/or scripts developed in house, as well as any procured application add-ons or components of commercially available software that has been tailored or customized beyond what the vendor will support. Whatever the interpretation, Registered Entities should assure the process and definitions developed are well documented and implemented consistently.



Recommended Application Guidance – Deep Dive into Part 1.1.3. (continued)**3rd Party Tool Options (continued)****Manual Options Continued**

Firmware-based Cyber Assets do not typically support the installation of custom software; therefore, this attribute may not be applicable to those types of devices. Registered Entities may choose to define and record an affirmative value to indicate this condition, such as 'N/A', 'not applicable', 'none', 'firmware-based only', etc. as opposed to a null or blank field in a manually maintained baseline.

Programmatically defining how this attribute is documented helps assure clarity that the attribute was evaluated and understood to be irrelevant and can prevent confusion or the misperception of an incomplete baseline.

Tip:	For Firmware-based Cyber Assets, if there is no custom software (including version), established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.
Lessons Learned:	Registered Entities should consider establishing standardized practices for development, registration, and path used to house custom software, programming code, and/or scripts to help assure monitoring practices include custom software. This can help prevent oversights that may place Registered Entities at odds with baseline configuration change and update requirements and compliance timeframes. It can also assure the Registered Entity can monitor for and detect unauthorized changes to maintain compliance with CIP-010-2 Requirement R2 Part 2.1.
Evidence:	Recommended evidence to retain could be, but is not limited to, text file outputs from commands or screenshots from a directory, registry, or locally installed utility of the commercially available or open-source application software. Assure evidence captured is sufficient to demonstrate compliance. Material attributes to consider including are: date information to demonstrate when it was established, the unique ID of the Cyber Asset, and a check to assure that material information is not truncated. Additionally, Registered Entities may want to consider developing and retaining any methodology documentation used to demonstrate how the inventory of custom software was determined.
Exhibits:	See Exhibit F: Part 1.1.2. & 1.1.3 – Installed Commercial or Open-source Software (Manual Options) for a sample batch script to 'Export Installed Programs'
Operational Controls Samples:	See Operational Controls Samples for Manual Options under 1.1.



CIP-010-2, REQUIREMENT R1, PART 1.1. – DEVELOPING BASELINES

Analysis, Part 1.1.4. – Logical Network Accessible Ports

Requirement Language (intentionally abbreviated to Part 1.1.4.)		
CIP-010-2 Table R1 – Configuration Change Management		
Part	Applicable Systems	Requirements
1.1	High and Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following item: 1.1.4. Any logical network accessible ports;
Evaluation		
Objective:	<p>The objective of Requirement R1 Part 1.1.4. is to identify and document any logical ports that are network accessible on applicable Cyber Assets to assure:</p> <ul style="list-style-type: none"> • Effective inventory, vulnerability mitigation, and risk management for routable communications via the network interface • During normal operations: <ul style="list-style-type: none"> ○ The presence and expected state of, and operational need⁹ for logical network accessible ports is clearly understood for personnel responsible for, implementing, supporting, and maintaining the applicable Cyber Assets, ○ Changes to network accessible logical ports trigger change control processes and authorizations, and ○ Configuration management and monitoring processes are inclusive of needed network accessible logical ports and designed to detect unauthorized changes. 	
Value Proposition:	<p>There are several benefits to tracking logical network accessible ports that collectively provide compliance, security, and reliability value. Documenting the approved and expected logical network accessible ports tracks the initial state of installation, and has the following additional benefits:</p> <ol style="list-style-type: none"> 1. Effectively managing documentation to track logical network accessible ports serves to provide awareness of the operational need for the routable protocol configurations within an ESP and its network connected systems, applications, or software that rely on specified ports or ranges for data communication. Knowledge of the need for logical 	

⁹ While CIP-010-2 Requirement R1., Part 1.1, Attribute 1.1.4. does not prescribe maintaining the business or operational need within the baseline documentation, Registered Entities may want to consider synergies with the mandatory obligations of CIP-007-6 Requirement R1 that causes the determination of 'need', and potential opportunities to realize efficiency gains by leveraging one process or tool to accomplish both compliance obligations and alignment between related records. Conversely, see the [Tip](#) in the main section of Part 1.3 for a caution about documenting determination of need for logical network accessible ports.



Evaluation (continued)**Value Proposition:**

(continued)

network accessible ports and tracking changes helps assure Registered Entities have an intimate understanding of data communication needs and are able to make informed decisions to control the network accessibility of logical ports and the risk or vulnerabilities that accessibility may present to reliable operations.

2. Effectively managing documentation to track logical network accessible ports also serves to partially support mandatory regulatory obligations and evidence to comply with:
 - CIP-005-5 Requirement R1. For those environments that have External Routable Connectivity (ERC), documenting what logical ports are network accessible on applicable Cyber Assets supports processes to identify which communications must traverse the ESP to assure it flows through an identified EAP. It also provides a basis for determining required inbound and outbound data flows and the reason for that communication.
 - CIP-007-6 Requirement R1. Documenting network accessible logical ports supports processes to determine the need for ports and services and is an opportunity to reduce the attack surface by knowing to remove network accessibility if not needed.
 - CIP-007-6 Requirement R2. Documenting what logical ports are network accessible supports processes to evaluate vulnerabilities associated to security patch releases, which in turn assists SMEs in identifying mitigating activities to reduce the risk of potential compromise through vulnerable logical network accessible ports.
 - CIP-010-2 Requirement R1 Parts 1.2 – 1.5 by helping to assure:
 - Prior to the change in network accessibility of logical ports or ranges
 - Authorization and documentation for changes to network accessibility of logical ports or ranges is completed pursuant to Requirement R1 Part 1.2,
 - Security control impact assessments are evoked pursuant to Requirement R1 Part 1.4, and
 - Controlled functionality testing procedures are executed for applicable high impact Cyber Assets/Systems pursuant to Requirement R1 Part 1.5
 - Following the implementation of custom software changes
 - Post-change security controls testing procedures are evoked pursuant to Requirement R1 Part 1.4, and
 - Established baselines are brought up-to-date to reflect actual needed network accessible logical ports and/or ranges pursuant to Requirement R1 Part 1.3
 - CIP-010-2 Requirement R2 for applicable high impact Cyber Assets/ Systems. Documenting what logical ports are network accessible supports processes and controls to detect, identify, respond, and/or recover from unintentional or unapproved changes, thereby reducing the volume of uncontrolled changes and minimizing the risk of causing instability or inoperability of Cyber Assets needed to support safe, secure, resilient, and reliable operation of the BES.



Recommended Application Guidance – Deep Dive into Part 1.1.4.

3rd Party Tool Options

A 3rd Party Tool may be able to automatically gather the Cyber Asset's network accessible ports utilizing several different techniques. The methods depend on the Cyber Asset type and capabilities.

For operating system based Cyber Assets, several methods may gather network accessible ports. The environment must be understood to accurately gather information. In Microsoft Windows operating system environments, a 3rd Party Tool may use the netstat command, but the netstat command will not accurately provide "logical network accessible" ports baselines per the requirement if the Windows Firewall feature or a 3rd party host-based firewall program is implemented. A host-based firewall may only allow some or none of the ports to be network accessible. To get an accurate baseline, the 3rd Party Tool needs to query the program controlling the firewall rules.

Some 3rd party programs can run on the local host to gather ports open to the network, but they do not typically consider ports blocked by a host-based firewall.

Another method to gather the network accessible port information is using a network scanning tool such as nmap to scan the baseline target host from another system. Some 3rd Party Tools allow use of additional programs like nmap; this is not without pitfalls. If this method alone is chosen to gather network accessible port baseline information, some logical network accessible ports may be missed. A host-based firewall may block ports from the scanning host if the scanning tool IP address is not in the access list for the all port based rules. If using network port scanning tools, verify host-based firewall rules allow the IP address of the host performing the scan so network accessible ports can be identified.

Even with the ports allowed by the target host, some ports may not be identified. UDP ports are notorious for not being reliably identified in network scans due to the nature of UDP. Some scanning programs are configured by default to only scan well known TCP and UDP ports. Make sure all 65535 TCP and UDP ports are scanned. Due to the way UDP is written and depending on how the application behind the service works, ports used for ntp, syslog, or SNMP deployed in a listen only mode may never be identified in a network scan but are open. Point being, several methods of analysis may need to be used on the target host to get an accurate list of network accessible ports. Using more than one method can produce a better network accessible ports baseline.

Other operating systems may also employ host-based firewall technology or IP access list capabilities, so the same precautions apply. Most network switches, routers, and firewalls can limit access to their management console to specific hosts. In this case, allow access from the host to the network scanning program. A service may be disabled on a system, but the network port associated with the service may remain open. Performing a network scan against the system may identify this issue.

For firmware based Cyber Assets, running an internal command to gather the network accessible port information may not be possible. A network scanning device can identify network accessible ports on some of these devices. However, a network scanning program may not identify services like ntp, syslog, or SNMP so the Cyber Assets configuration should be examined. Examples are: netstat commands for Windows (netstat -abon¹⁰ and Linux (netstat -atunp) based Cyber Assets

¹⁰ The 'b' flag in the netstat -abon command applies to Windows XP and newer versions of Windows.



Recommended Application Guidance – Deep Dive into Part 1.1.4. (continued)	
3rd Party Tool Options (continued)	
Tip 1:	Consider installing an agent on a Cyber Asset on the same network segment (subnet) as the Cyber Assets to be scanned. This will reduce issues with network equipment access lists preventing scanning of Cyber Assets.
Tip 2:	Consider the location of the Cyber Asset performing a network scan to the Cyber Asset being scanned. Scanning traffic that is inspected by an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) may cause excessive alerts or the scanning traffic may be dropped completely.
Tip 3:	For 3rd Party Tools with the capability to run a port scan, such as nmap, a planned outage may be needed since the scan could affect the network communication or the functionality of the Cyber Asset. Certain protocols, such as GOOSE, can be affected and cause relay tripping, so a planned outage may be needed if alternatives to scanning are not available for the Cyber Asset. Delay parameters may be needed to prevent Denial of Service attacks.
Lessons Learned 1:	Depending on the sophistication of the 3rd Party Tools you are using, some may interpret results as false positives and others may simply report on the native conclusion from the tool. For example, nmap (while not a 3rd Party Tool) scans may report a status of open-filtered for UDP ports. This may mean the port is blocked by a host firewall policy, or perhaps the scan timeout was too short, and a result could not be achieved. These are two potential reasons, yet not all reasons why this result may occur. When utilizing 3rd Party Tools, be conscious of potential false positives and the potential need to utilize multiple methods and/or perform further investigation to confirm the actual status.
Lessons Learned 2:	The use of network scanning tools can adversely impact the Cyber Asset. As an example, these tools can trip or overwhelm resources on relays in a transmission or generation facility. Also consider potential adverse effects on typical IT infrastructure. Running scans in a test environment helps identify adverse effects that could compromise functionality within a production environment.
Lessons Learned 3:	Registered Entities may choose to add other attributes to established baselines and/or leverage other programs that are used comply with CIP-007-6 to achieve the CIP-010-2 baselines. There are similarities between CIP-007-6 Requirement R1 and the baselining attribute in CIP-010-2 Requirement R1 Part 1.1.4; however, there are also nuances like the presence of the concept for ‘services’ in one requirement and not the other that could make it unclear that entities should be baselining both ports and services. This is supported by the fact that both CIP-007-6 R1 Part 1.1 and CIP-010-2 R1 Part 1.1 1.1.4 are directly connected and referenced in the Guidelines and Technical Basis of CIP-010-2, which reads, “If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. This nuance means strict compliance to CIP-010-2 Requirement R1 Part 1.1.4 does not achieve full compliance with CIP-007-6 Requirement R1 & R2. Registered Entities are not expected to track things that are not explicitly included in 1.1, however, the baseline could be used to support compliance with related requirements like these.



Recommended Application Guidance – Deep Dive into Part 1.1.4. (continued)**3rd Party Tool Options (continued)****Lessons Learned 4:**

If a network scanning tool is used to identify network accessible ports, consider:

- Verifying all network interfaces are scanned, physical and virtual. Some systems can only open ports on specific interfaces, so scanning just one interface may not produce an accurate baseline. Some systems use VLAN trunk ports, so a network scanning system will need access to all of the VLANs.
- Having an agent on the same network segment as the intended target host(s) to accurately perform network scans. Performing network scans through a firewall can produce inaccurate results and generate excessive logs.

Lessons Learned 5:

For any dynamic ports, the port range needs to be included. Some Cyber Asset types require a predefined port range that is used on demand for proper operation. These ports are typically not persistently network accessible and therefore may not appear in scan results. Typical systems that use dynamic ports are Windows or Linux and UNIX variants, however some firmware-based Cyber Assets may also require dynamic ports. As an example, for Windows-based machines, the following netsh commands captures the dynamic port range:

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

Vendor manuals may be an initial source to help identify the dynamic port range. Contacting the vendor and/or running multiple test scans, preferably in a non-production environment, may provide extra assurance that dynamic ranges are identified and documented.

As an example, one manufacturer's appliances do have commands that are supposed to list the open network ports on its interfaces, but it has been observed that the commands do not reliably return all the network accessible ports. Having an in depth understanding of what each tool is capable of to assure the intended outcomes is achieved. Entities may want to consider implementing practices that rely on at least two tools to help provide this assurance, and it is recommended that if these commands are used, a network scan should also be performed used to validate the data.

Commands for identifying open network TCP and UDP ports:

- sh asp table socket
- sh local-host
- sh conn



Recommended Application Guidance – Deep Dive into Part 1.1.4. (continued)	
3rd Party Tool Options (continued)	
Evidence:	<p>Recommended evidence to retain could be, and is not limited to, reports, exports, or in-system database records or logs of the logical network accessible ports. Assure the evidence captured is sufficient to demonstrate compliance.</p> <p>Consider including the following attributes in the records retained to demonstrate compliance, as well as quality control mechanisms to help assure material information is present, legible, and not truncated:</p> <ul style="list-style-type: none"> • Date/Time demonstrating when 3rd Party Tools outputs were generated, whether within the in-system log or exported as separate evidentiary artifact • Date/Time demonstrating when each baseline was established/approved • Unique ID of each applicable Cyber Asset for traceability to the baseline and assurance the full population is covered <p>Types of evidence to retain could include, but is not limited to, <i>system-generated</i> outputs of ports and services from 3rd party scanning tools or commands, such as utilities like netstat, TCPdump, nmap, etc.</p> <p>Some 3rd Party Tools that interrogate systems for open ports and capture logs store records within the tool; these tools can be utilized to retain evidence.</p> <p>Other forms of evidence may supplement scanning outputs. These supplements include but are not limited to host-based firewall ports configurations or interface-level configurations</p>
Exhibits:	See Exhibit G: Part 1.1.4. – Logical Network Accessible Ports (3rd Party Tool Options) for an example of a <i>system-generated</i> report.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. During the software evaluation processes, trial versions of 3rd Party Tools are tested for the ability to gather evidence for Part 1.1.4 to assure procured products meet mandatory regulatory obligations.
Manual Options	
<p>Even if a BES Cyber System does not have External Routable Connectivity, applicable Cyber Assets may use a routable protocol within the ESP. For those Cyber Assets, network assessable ports need to be identified.</p> <p>Applicable Cyber Assets with enabled routable interfaces that are not connected to a network or another applicable Cyber Asset using a routable protocol may not have network-accessible, logical ports upon initial implementation. This depends on the hardware profile (i.e. presence of ethernet ports) and the physical or logical controls (or lack thereof) applied to any routable hardware interfaces. Implementing controls reduces the risk that interfaces become connected to a network which requires a baseline. Registered Entities could disable the routable interface, implement a port blocker, attach tamper tape, or remove the routable interface hardware (if technically feasible).</p>	



Recommended Application Guidance – Deep Dive into Part 1.1.4. (continued)	
3rd Party Tool Options (continued)	
Manual Options Continued	
Tip 1:	For manually executed port scanning, such as nmap, a planned outage may be needed since the scan could affect the network communication or the functionality of the Cyber Asset. Certain protocols, such as GOOSE, can be affected and cause relay tripping, so a planned outage may be needed if alternatives to scanning are not available for the Cyber Asset. Delay parameters may be needed to prevent Denial of Service attacks.
Lessons Learned 1:	<p>Depending on the options available when executing a manual solution, some scanning commands may interpret results as false positives and others may simply report on the native conclusion the command is configured to return. For example, nmap scans may report a status of open-filtered for UDP ports. This may mean the port is blocked by a host firewall policy, or the scan timeout was too short, and a result could not be achieved.</p> <p>These are two potential reasons, yet not all reasons why this result may occur. When utilizing certain port status commands, be conscious of potential false positives and the potential need to utilize multiple methods and/or perform further investigation to confirm actual status.</p>
Lessons Learned 2:	Registered Entities may choose to add other attributes to established baselines and/or leverage other programs that are used to comply with CIP-007-6 to achieve the CIP-010-2 baselines. There are similarities between CIP-007-6 Requirement R1 and the baselining attribute in CIP-010-2 Requirement R1 Part 1.1.4; however, there are also nuances like the presence of the concept for ‘services’ in one requirement and not the other. This nuance means strict compliance to CIP-010-2 Requirement R1 Part 1.1.4 does not achieve full compliance with CIP-007-6 Requirement R1 & R2. Registered Entities are not expected to track things that are not explicitly included in 1.1, however, the baseline could be used as information that supports compliance with related requirements like these
Evidence:	Evidence to retain could include, but is not limited to, text-based outputs of ports and services from manually executed commands, such as utilities like netstat, TCPdump, nmap, etc. Other supplemental forms of evidence for scanning command outputs could include, but are not limited to, host-based firewall ports configurations or interface-level configurations. Material attributes to consider including are date information to demonstrate when it was established, the unique ID of the Cyber Asset, and a check to assure that material information is not truncated.
Exhibits:	See Exhibit H: Part 1.1.4. – Logical Network Accessible Ports (Manual Options) for examples of netstat and nmap scripts.
Operational Controls Samples:	See Operational Controls Samples for 3rd Party Tools under 1.1.



CIP-010-2, REQUIREMENT R1, PART 1.1. – DEVELOPING BASELINES

Analysis, Part 1.1.5. – Applied Security Patches

Requirement Language (intentionally abbreviated to Part 1.1.5.)		
CIP-010-2 Table R1 – Configuration Change Management		
Part	Applicable Systems	Requirements
1.1	High and Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Develop a baseline configuration, individually or by group, which shall include the following item: 1.1.5. Any security patches applied
Evaluation		
Objective:	<p>The objective of Requirement R1 Part 1.1.5. is to identify and document any security patches applied to applicable¹¹ Cyber Assets to assure:</p> <ul style="list-style-type: none"> • Effective vulnerability mitigation, and risk management of running OS/FW versions, intentionally installed commercial applications and/or open source software, and vulnerable enabled logical ports or services, including but not limited to logical network accessible ports. • During normal operations: <ul style="list-style-type: none"> ○ The expected state of applied security patches is clearly understood for personnel responsible for implementing, supporting, and maintaining patch management tasks ○ Changes to applied security patches trigger change control processes and authorizations, and ○ Configuration management and monitoring processes are inclusive of installed applied security patches, and designed to detect unauthorized changes to patch installations 	
Value Proposition:	<p>There are several benefits to tracking applied security patches that collectively provide compliance, security, and reliability value. Documenting the approved and expected security patch level tracks the initial state of installation, and has the following additional benefits:</p> <ol style="list-style-type: none"> 1. Effective management of documentation that tracks applied security patches serves to partially support mandatory regulatory obligations to comply with CIP-007-6 Requirement R2. By recognizing this synergy, Registered Entities can realize efficiency gains by leveraging one process or tool to accomplishing both compliance obligations. 	

¹¹ The use of the term applicable within this section refers to the Cyber Asset listings within the Applicable Systems column of each Requirement Part of each Table relevant to CIP-010-2 Requirements R1 & R2.



Evaluation (continued)	
Value Proposition: (continued)	<p>Applied security patches tracking supports CIP-007-6 Requirement R2 compliance activities and security objectives when used to identify and document patch sources, ascertain applicability, and streamline review/assessment of patch releases in scope for the Registered Entity, and making informed decisions to mitigate vulnerabilities.</p> <ol style="list-style-type: none"> 2. Similarly, the benefit of documented applied security patches is not just maintaining compliance; it also provides security-risk reduction and the added business value of supporting reviews of imminent or released upgrades, fixes, and feature enhancements that may improve operational stability or capability of the system. 3. Effectively managing applied security patches tracking documentation also serves to position Registered Entities for successful performance of the remaining mandatory regulatory obligations to comply with CIP-010-2 Requirement R1 Parts 1.2 – 1.5 by helping to assure: <ul style="list-style-type: none"> ○ Prior to the implementation or removal/rollback of security patches <ul style="list-style-type: none"> ● Authorization and documentation for custom software changes is completed pursuant to Requirement R1 Part 1.2, ● Security control impact assessments are evoked pursuant to Requirement R1 Part 1.4, and ● Controlled functionality testing procedures are executed for applicable high impact Cyber Assets/Systems pursuant to Requirement R1 Part 1.5 ○ Following the implementation of custom software changes <ul style="list-style-type: none"> ● Post-change security controls testing procedures that assure installed security patches are applied are evoked pursuant to Requirement R1 Part 1.4, and ● Established baselines are brought up-to-date to reflect actual installed and applied patches pursuant to Requirement R1 Part 1.3 4. Effectively managing applied security patches tracking documentation also serves to partially support mandatory regulatory obligations to comply with CIP-010-2 Requirement R2 for applicable high impact Cyber Assets/ Systems. Documenting what Applied security patches are installed supports processes and controls to detect, identify, respond, and/or recover from unintentional or unapproved changes, thereby reducing the volume of uncontrolled changes and minimizing the risk of causing instability or inoperability of Cyber Assets needed to support safe, secure, resilient, and reliable operation of the BES.
Recommended Application Guidance – Deep Dive into Part 1.1.5.	
3rd Party Tool Options	
<p>Automated 3rd Party Tools can assist baselining applied security patches for operating system based Cyber Assets. They typically pull information from system configuration files. 3rd Party Tools should be able to gather, store, and produce a report on system security patches.</p> <p>For firmware based Cyber Assets, the security patch level attribute must be documented even where it is equal to the firmware version documented as a function of attribute 1.1.1. Registered Entities can consider</p>	



Recommended Application Guidance – Deep Dive into Part 1.1.5. (continued)**3rd Party Tool Options (continued)**

several options for how to record this value. A Registered Entity could choose to record this value twice or alternatively, could choose to use a pointer from one attribute to the other indicating the installed firmware version is equal to the applied security patches. Regardless of if the attribute is tracked individually or in a grouping by another common attribute with pointers (like but not limited to, Cyber Asset class and firmware version), it is the Registered Entity's responsibility to assure sufficient evidence for all baseline attributes to be tracked to the most granular item (i.e. applicable Cyber Asset and individual attribute value).

Tip: Although this requirement is not typically relevant to firmware based Cyber Assets that only have one firmware applied at a time which is already tracked for 1.1.1., established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.

Lessons Learned 1: Registered Entities may choose to add other attributes to established baselines and/or leverage other programs that are used to comply with CIP-007-6 to achieve the CIP-010-2 baselines. There are similarities between CIP-007-6 Requirement R2 and the baselining attribute in CIP-010-2 Requirement R1 Part 1.1.5; and while the baseline attribute supports the successful execution of related security patch management obligations, these additional obligations for documented 'patch sources', 'security patch release assessments', and 'installation or mitigation actions' go beyond tracking the applied patch level. This nuance means strict compliance to CIP-010-2 Requirement R1 Part 1.1.5 does not achieve full compliance with CIP-007-6 Requirement R2. Registered Entities are not expected to track things that are not explicitly included in 1.1, however, the baseline could be used to support compliance with related requirements like these.

Lessons Learned 2: As the CIP Standard evolved, nuances between the language for the security patching requirement of CIP-007-3 R3 and CIP-007-6 R2 were introduced, and this may cause unintended consequences in BIOS-level software updates that may affect the 1.1.5 baseline attribute, particularly if a BIOS-level security patch is identified pursuant to CIP-007-6 R2.1 for cyber security patches. The wording of the CIP-007-6 standard changed from version 3 to version 6; version 3 used to qualify security patches with the word "software" whereas version 6 has this word removed. Including hardware-based security patch sources in this program creates a defensible position for this nuance.

Consider the situation where a Microsoft Windows or Linux based computer system (workstation or server) BIOS has been issued a security update. If this firmware was not previously tracked as part of requirement 1.1.1 it should be tracked as part of 1.1.5 if the security update is applied. Identifying, tracking, evaluating, and installing cyber security patches for applicable Cyber Assets is a requirement of CIP-007-6.

Lessons Learned 3: Overreliance on technology could have unintended consequences without intimate knowledge of varied Cyber Assets. The technical method used to retain security patch installation history may vary by Cyber Asset. To assure needed evidence is captured, Registered Entities are encouraged to gain comprehensive familiarity with how each unique system records applied security patches, and how subsequent patch application can affect evidence and the ability to prove compliance.



Recommended Application Guidance – Deep Dive into Part 1.1.5. (continued)	
3rd Party Tool Options (continued)	
<p>Lessons Learned 3:</p> <p>Continued</p>	<p>As one example, consider a Windows-based system where an applicable security patch is applied; approvals and baseline updates occur within the compliance timeframes. A system registry entry proves the installation, so no additional evidence outside the Cyber Asset is captured. Six months pass, and another applicable security patch is applied, and the installation removes the need for the other registry entry, so the system removes it.</p> <p>During audit, the Cyber Asset or Security Patch is sampled, and an output of the registry is provided as evidence and does not include the first patch. This does not mean the Registered Entity is non-compliant; however, it may mean it is more difficult to prove. In this scenario the Registered Entity may need to provide supporting vendor documentation to demonstrate what happened. Dated change records may need to be provided in substantiation that the patch was installed within the 35 calendar days of the patch assessment. Registered Entities may want to consider implementing safeguards to avoid this predicament. One potential approach to could be to snapshot baseline configuration on a 30-calendar day interval and archive it off for future use. Another alternative might be to implement a practice to export, screenshot, or otherwise capture point-in-time registry information following patch installation as a part of that process.</p>
Evidence:	<p>Recommended evidence to retain could be, and is not limited to, reports, exports, or in-system database records or logs of the OS/FW version. Assure the evidence captured is sufficient to demonstrate compliance.</p> <p>Consider including the following attributes in the records retained to demonstrate compliance, as well as quality control mechanisms to help assure material information is present, legible, and not truncated:</p> <ul style="list-style-type: none"> • Date/Time demonstrating when 3rd Party Tools outputs were generated, whether within the in-system log or exported as separate evidentiary artifact • Date/Time demonstrating when each baseline was established/approved • Unique ID of each applicable Cyber Asset for traceability to the baseline and assurance the full population is covered
Exhibits:	<p>See Exhibit I: Part 1.1.5. – Applied Security Patches (3rd Party Tool Options) for an example of a <i>system-generated</i> report.</p>
Operational Controls Samples:	<ol style="list-style-type: none"> 1. See Operational Controls Samples for 3rd Party Tools under 1.1. 2. During the software evaluation processes, trial versions of 3rd Party Tools are tested for the ability to gather evidence for Part 1.1.5 to assure procured products meet mandatory regulatory obligations.



Recommended Application Guidance – Deep Dive into Part 1.1.5. (continued)

3rd Party Tool Options (continued)

Manual Options

Batch scripts can capture security patches applied to Microsoft Windows and Linux devices to a text file. Manually recording outputs from native, local utilities that track installed security patches is another approach.

For firmware based Cyber Assets, the security patch level attribute must be documented even where it is equal to the firmware version documented as a function of attribute 1.1.1. Registered Entities can consider several options for how to record this value. A Registered Entity could choose to record this value twice or alternatively, could choose to use a pointer from one attribute to the other indicating the installed firmware version is equal to the applied security patches. Regardless of if the attribute is tracked individually or in a grouping by another common attribute with pointers (like but not limited to, Cyber Asset class and firmware version), it is the Registered Entity’s responsibility to assure sufficient evidence for all baseline attributes to be tracked to the most granular item (i.e. applicable Cyber Asset and individual attribute value).

Tip: Although this requirement is not typically relevant to firmware based Cyber Assets that only have one firmware applied at a time which is already tracked for 1.1.1., established baselines could include documentation identifying this as not applicable to demonstrate understanding of system capabilities.

Lessons Learned 1: Registered Entities may choose to add other attributes to established baselines and/or leverage other programs that are used to comply with CIP-007-6 to achieve the CIP-010-2 baselines. There are similarities between CIP-007-6 Requirement R2 and the baselining attribute in CIP-010-2 Requirement R1 Part 1.1.5; and while the baseline attribute supports the successful execution of related security patch management obligations, these additional obligations for documented ‘patch sources’, ‘security patch release assessments’, and ‘installation or mitigation actions’ go beyond tracking the applied patch level.

This nuance means strict compliance to CIP-010-2 Requirement R1 Part 1.1.5 does not achieve full compliance with CIP-007-6 Requirement R2. Registered Entities are not expected to track things that are not explicitly included in 1.1, however, the baseline could be used as information that supports compliance with related requirements like these.

As the CIP Standard evolved, nuances between the language for the security patching requirement of CIP-007-3 R3 and CIP-007-6 R2 were introduced, and this may cause unintended consequences in BIOS-level software updates that may affect the 1.1.5 baseline attribute, particularly if a BIOS-level security patches is identified pursuant to CIP-007-6 R2.1 for cyber security patches. The wording of the CIP-007-6 standard changed from version 3 to version 6; version 3 used to qualify security patches with the word “software” whereas version 6 has this word removed. Including hardware-based security patch sources in this program creates a defensible position for this nuance.



Recommended Application Guidance – Deep Dive into Part 1.1.5. (continued)	
Manual Options (continued)	
Lesson Learned 1: (continued)	Consider the situation where a Microsoft Windows or Linux based computer system (workstation or server) BIOS has been issued a security update. If this firmware was not previously tracked as part of requirement 1.1.1 it should be tracked as part of 1.1.5 if the security update is applied. Identifying, tracking, evaluating, and installing cyber security patches for applicable Cyber Assets is a requirement of CIP-007-6.
Evidence:	Evidence may include but is not limited to, <i>system-generated</i> outputs of security patching levels or screenshots of commands executed on an applicable asset. System evidence may be retained in a centralized patching management system that either maintains a database of hosts and installed patches or can query a host for installed security patches. Most of these tools can provide reports that may be used as evidence to demonstrate baselines were updated within the 30-calendar day requirement. Like 1.1.1, evidence may also be captured for firmware only devices through inspection and manual recording through the methods described in 1.1.1. Material attributes to consider including are date information to demonstrate when it was established, the unique ID of the Cyber Asset, and a check to assure that material information is not truncated.
Exhibits:	See Exhibit J: Part 1.1.5. – Applied Security Patches (Manual Options) for a sample export of Windows PC applied security patches.
Operational Controls Samples:	See Operational Controls Samples for 3rd Party Tools under 1.1.



CIP-010-2, REQUIREMENT R1 – CONFIGURATION CHANGE MANAGEMENT

Analysis, Part 1.2. – Authorizing & Documenting Baseline Deviations

Requirement Language			
CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.2	High and Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: <ul style="list-style-type: none"> • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Evaluation			
Objective:	The objective of authorizing and documenting changes to baseline configurations pursuant to Requirement R1 Part 1.2 is to assure baseline deviations are intended, coordinated, and historically tracked. There are two distinct components of this requirement, authorize and then document. The authorization should occur prior to the baseline change, and sufficient information about the intended baseline change should be provided to the authorizer prior to making the authorization. Documentation of this authorization provides accountability and reasonable assurance that the change management process was executed. The second objective of this requirement is to document the baseline change. This ties to Requirement R1 Part 1.3 but is different in that Part 1.2 is to make sure the actual change was described to the authorizer and collect evidence supporting this conclusion.		
Value Proposition:	Configuration change management is paramount to maintaining secure cyber systems. Without tracking configuration changes to a Cyber Asset, it would be difficult to know when a change was supposed to be made and that the changes were properly vetted. In a secure environment changes should be vetted and not applied ad hoc. Without a proper configuration change management process tracking these tasks can be difficult. <p>Consider a scenario where one analyst modifies attributes of a Cyber Asset such as installing a new software package that opens communication ports to the network. Later a vulnerability is identified with the newly installed software.</p> <p>Change management allows other analysts to ascertain why and when the software was installed, who to contact to discuss the importance of the software in case it should be removed or operated with limited functionality to mitigate the vulnerability in the absence of the analyst</p>		



Evaluation (continued)	
<p>Value Proposition:</p> <p>(continued)</p>	<p>that originally installed the software. Change management can also aid in determining how long a Cyber Asset could be affected by the vulnerability.</p> <p>In the case where a change to a Cyber Asset is discovered, authorizations and documented, change management records provide value when investigating if the change was intended or possibly malicious. If the detected change is not in the change management system Registered Entities may want to consider if the Cyber Security Incident Response Plan (CIP-008-5) needs to be activated to determine if there has been a Cyber Security Incident.</p>
Recommended Application Guidance – Potential Approaches	
<p>Part 1.2 requires changes that deviate from an existing baseline configuration be authorized and documented. There are two distinct components to this requirement, authorize and document.</p> <p>Depending on how a Registered Entity has implemented baselines, the change process may provide the flexibility to request authorization of baseline changes for individual Cyber Assets, a group of ‘like’ Cyber Assets (i.e., same make, model and firmware), or a group of Cyber Assets common to a given activity (i.e., construction projects). Searchability and traceability of records are a consideration for Registered Entities to make when defining how to request and authorize changes.</p> <p>Consider including any limiting factors or time constraints associated to mandatory compliance timeframes. If the change is associated to security patching and a mitigation plan has not been established or revised and approved, the process should include controls that assure the 35 calendar days to install the security patch is not exceeded.</p> <p>When authorizing and documenting an individual change request consider whether multiple change request tickets should be created for each device requiring a baseline change or if a single change request ticket should be created that identifies all devices with the same baseline change. There are advantages and disadvantages to each approach and both options should be considered.</p>	
Tip 1:	<p>Whatever solution is chosen to authorize and document the approval for configuration baseline changes, Registered Entities ease of use and user friendliness can be key to success, and consideration of repeatability, consistency, and sustainability in the processes and tools may streamline execution of the process</p>
Tip 2:	<p>Consider designating delegates for approvals of change requests. There may be situations when the primary approver(s) is not available due to planned and unplanned absences. Having a process to delegate the approvals of change requests allows for continuity of the overall change management process.</p>
Lessons Learned 1:	<p>As part of the change management process consider documenting the types of changes to a Cyber Asset that are routine and technically do not affect system ‘baselines’ as defined in the Standard. This can provide guidance to support personnel as to when CIP-010-2 Part 1.4 comes into play and can also help make informed decisions about change types that could cause unintended consequences of causing violations with other CIP Requirements. Envision a scenario where an IP Address configuration is changed on a BCA, it could:</p> <ul style="list-style-type: none"> • Prevent or adversely affect Malware prevention signature or pattern updates,



Recommended Application Guidance – Potential Approaches (continued)	
<p>Lessons Learned 1:</p> <p>Continued</p>	<ul style="list-style-type: none"> • Disrupt configuration monitoring server/client communications, • Inhibit the ability to successfully send security event information, • Negate EAP controls by logically relocating the BCA to a subnet outside of the ESP, removing it from a protected environment, and potentially exposing the BCA to direct Interactive Remote Access. • Disassociate the BCA from inventory records, the BCS, and the established baseline if the IP Address is used as the correlating unique ID • Introduce a duplicate IP address in a critical environment causing operational instability or unavailability of other BCAs
<p>Lessons Learned 2:</p>	<p>Though the flexibility may exist within the regulation, Registered Entities may also want to carefully consider if including programmatic provisions for pre-authorization¹² of standardized cyclical changesⁱ to baselines are allowable within its environment.</p> <p>Registered Entities who choose to have standing approvals for routine changes to streamline processes, are cautioned to be mindful in the approach to prevent unintended consequences on the operating environment and/or misuse (or over allowance/extended use) of practices like this that could affect an entity’s ability to comply. Consider that CIP-010-2 Requirement R1 Part 1.3 has a 30-calendar day timeframe for baseline updates, and pre-authorized changes with cycles in excess of 30 calendar days could confuse or convolute the completion date and pose compliance risk in the timing associated to baseline updates.</p> <p>If choosing to establish programmatic provisions for pre-authorization of standardized cyclical changes to baselines as allowable, it may be prudent to establish supporting processes for the periodic review and reauthorization of standardized cyclical changes.</p> <p>One value of requiring an authorization process is the opportunity it provides for consideration of point in time interdependencies, resource constraints, competing activities, or other operational circumstances that may be a factor significant enough to cause the change to be deferred. This value could be lost is using practices to pre-authorize changes.</p>
<p>Lessons Learned 3:</p>	<p>Consider including the handling of emergency situations in change management process documentation. This can help guide support staff during situations where the importance of getting a critical system fixed is paramount.</p> <p>Compliance and reliability may both be maintained with a flexible process. Consider allowance of verbal change request approvals to system changes when in emergency situations. These approvals should typically be very rare and should be documented as soon as practical after addressing an emergency.</p>

¹² The CIP SMET engaged in thoughtful debate about the inclusion of this concept and chose to include it as a Lessons Learned to caution Registered Entities of the complexities to successfully implement these types of provisions in manner that is not at variance with mandatory obligations. While there may be ways to achieve compliance using this approach, interpretations may vary, and it may be challenging to demonstrate to an auditor that this practice carries a level of rigor commensurate with the intent of the Requirements. For these reasons, this practice is not generally recommended, and the CIP SMET encourages Registered Entities to consider if the practice is worth the operational or compliance risk and the scrutiny of interpretive debate.



Recommended Application Guidance – Potential Approaches (continued)	
Lessons Learned 4:	Where verbal approval is permitted for emergencies to assure reliability and security first, consider implementing internal controls to govern this process via monitoring and review of frequency and volume of emergency changes to provide reasonable assurance that the emergency change process is not being abused as a vehicle to bypass pre-approvals, or constituting undue urgency as a substitute for coordination and planning. Metrics and periodic reviews to of these measurements can help assure that poor planning is not used to constitute false urgency that can lead to operational or security risk if left unchecked.
Evidence:	Evidence may include but is not limited to, change request record and associated authorization from the ticketing system, form authorizing the change, or meeting notes authorizing the change.
Operational Controls Samples:	<p>Change processes include steps for the assessment of baseline attributes and the identification of baseline configuration deviations. Upon the identification of a need to change baseline configuration, the change process directs SMEs on how to obtain authorization.</p> <p>On a cycle predefined by the Registered Entity, a Change Advisory Board meets to review planned changes completed within the previous cycle and response actions to conditions that required emergency changes. Change records are reviewed for authorizations, any conditions where baseline changes occurred and expected authorizations were not documented are identified and provided to cybersecurity for investigation and resolution.</p>
3rd Party Tool Options	
<p>This type of authorization request could be processed through a change or work order management system to document the work and approvals. Some commercially available products are designed to perform change control and configuration management. The capability of these 3rd Party Tools varies depending on the tool you choose, and consideration of how to capture the pertinent information in each request and how to route the approval work and effectively document authorization is important.</p> <ul style="list-style-type: none"> • When it comes to identifying the parameters and scope of a configuration baseline change, the affected Cyber Assets and attributes being modified are key to capturing evidence demonstrating what was changed, vs what was authorized to be changed. 3rd Party Tools come with varied degrees of capability that a Registered Entity may want to consider. Some examples of these varied capabilities are: <ul style="list-style-type: none"> ○ Some tools are modular in nature where change requests can be linked to Cyber Assets within a database that is captured all within the same tool. ○ Others have system integration capabilities to leverage other tools, like an inventory management system that may house equipment information to connect the change request to Cyber Assets undergoing change. ○ Some operate in a more standalone manner supported by less sophisticated means, like manual data entry, to correlate change requests to Cyber Assets inventoried via another system or standalone means like a spreadsheet. • When it comes to authorizing changes to configuration baselines, the dates associated to the change, and information about the approver for the change are key to capturing quality records. This demonstrates when the approval occurred in relation to when the change was performed and can provide reasonable assurance that the person authorizing the change has the authority to do so. Depending on the tool chosen, there are varied levels of automation and features available to perform the authorization task and capture the approval record. 	



Recommended Application Guidance – Potential Approaches (continued)**3rd Party Tool Options (continued)**Approval workflow features or options:

- More mature tools may support automated workflow capabilities. Depending on the sophistication of the tool, it may contain predefined workflows for which personnel are assigned to predefined role, or it may be configurable to support customized workflows. These features often integrate with email functionality to notify responsible personnel as a change moves into a person's queue, and/or may even have the capability to consume an email as a response to an approval request, providing an additional mobility feature for the process.
- Where a 3rd Party Tool is designed specifically for change control, it is not uncommon for it to leverage industry accepted frameworks or standards like ITIL to define the type of change, phases of its lifecycle, and the approval workflow. Tools with configurable workflows are often based on a similar foundational practice that can serve as a template and come with additive features to customize it to an organization's process(es). Additional benefits of more mature tools like these are that they often consider standardized best practices or safeguarding concepts like Separation of Duties where approval workflows are concerned, and often incorporate technical controls of the tool.
- Sometimes this is accomplished using in-system tables or where approvers can be identified and correlated to change requesters by predefined relational data like reporting structure, departmental responsibility, system owner, or job function etc. These resource assignments can then be leveraged within the change request often through a drop-down menu for assignment, or even an automated look up based on other criteria the tool captures in the change request.
- Other systems may leverage system to system integration to other relational databases and may even link into other identity conscious systems to consume personnel data and validate reporting relationships or job duties between the change requestor and the approver as additional confidence that the person authorizing a change has the knowledge and authority to do so. As an example, a 3rd Party Tool may come with connectors to other commercially available Human Capital Management or Identity Access Management systems that may leverage Active Directory integration and then leverage a logged in users' authentication to control if the user can approve the change.

Approval queuing, monitoring, and alerting:

- Other tools that offer less sophistication may still have features that semi-automate approval workflow and documentation tasks. Some allow for the manual entry and assignment of approver names to display tasks in a manually monitored queue.
- Others leverage email address to assign work and often send a simple notification to the identified approval party. These systems may require the recipient of the notification to log in through a web portal or even a thick client to manually approve the request.

The simplest of 3rd Party Tools may be comprised of an online list or library without workflow capability where end users or groups of personnel are configured to receive alerts when a new item or a change to an existing item occurs. A manual process may be an option to support a solution like this to set expectations for the monitoring of alerts and the manual task to click on a link provided in the alert and to add approval comments into an online form.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Tip 1:	When using a 3rd Party Tool, often the applications and/or associated databases come with electronic versioning or audit history capabilities that can be used to demonstrate compliance.
Tip 2:	Consider incorporating provisions for emergency changes such that restoration of security and reliable operations may be prioritized and addressed unencumbered by administrative tasks associated to formal change control authorization and documentation practices. One potential approach could be to allow verbal approval and post change documentation and written authorization.
Tip 3:	Although a CIP Exceptional Circumstances (CEC) cannot be taken for compliance with Part 1.2, the criterion in the CEC definition may provide a starting point for when use of the emergency change process is acceptable.
Tip 4:	Consider implementing practices that employ the concept of separation of duties to prevent conditions where the implementer is also operating in the role of the approver. When segregating duties, also assure that personnel placed in an approver role are close enough to the operational activities or function to effectively assess the risk associated to the timing and content of the change.
Lessons Learned 1:	Registered Entities may want to consider defining what constitutes an emergency change, in addition to documenting and implemented monitoring and governance practices that provide reasonable assurance that emergency change processes are not used as a workaround to pre-planning for change.
Lessons Learned 2:	Registered Entities may want to consider defining what constitutes acceptable approval methods and processes that support obtaining authorization in conditions where the primary approver(s) is unavailable. One approach could be to leverage reporting structure to elevate to the leader of the approver that is unavailable; another could be to document implicit authority of the designated CIP Senior Manager (or delegates). Defining approvers by role or having a documented process for approvers to delegate backups is another consideration.
Evidence:	<p>Clear dated evidence of the approval of the baseline change should be maintained securely as compliance evidence. When using 3rd Party Tools, records could include in-system digital approvals, change version history, database audit logs or application journal entries, and/or workflow authorization records. Technical controls that log electronic approvals are typically date-stamped by the system or application to demonstrate authorizations occurred at the expected stage in the implemented change control process.</p> <p>Registered Entities may want to consider supplementing approval records with information out of the human capital management system to provide traceability to reporting structure and demonstrate that personnel who authorized baseline configuration changes operate in a role with the authority to do so.</p>
Exhibits:	See Exhibit K: Part 1.2. – Authorizing & Documenting Baseline Deviations (3rd Party Tool Options) for example of an automated approval workflow from a change management system.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Operational Controls Samples:	<ol style="list-style-type: none"> 1. On a cycle¹³ defined by the Registered Entity, the Change Advisory Board reviews a report from the 3rd Party Tool listing all detected baseline attribute changes and compares them to a report generated from the change management system to verify that authorizations exist for deviations to baselines for the cycle. Gaps are reported to incident responders who: <ol style="list-style-type: none"> a. Investigate and resolve any conditions where approvals for intended baseline changes do not exist, b. Investigate, report, and revert or mitigate, and document any conditions where unauthorized baseline changes are discovered.
Manual Options	
<p>Requirements 1.2 through 1.5 merge to form a repeatable cycle that is performed after the baseline is developed and each time a change to established baseline occurs. The baseline set for 1.1 serves as an input to the cycle and a reference throughout the execution and testing of the change.</p> <p>It is critical each person know their assigned roles in the process and vigilantly track their progress in a manual system. If there is a break in the manual system, there may not be safeguards to ensure timelines are met. In the below scenario, the Registered Entity leverages a request form and checklists to capture the request and approval information.</p>	
Tip 1:	In a manual process, it is helpful to have a section on a request form that allows the identified approver to mark their approval or denial on the form and the date. This identifies if requested changes should be carried out and documents the approval step for evidence.
Tip 2:	In a manual process, signatures can sometimes be difficult to read. It may be helpful to have fields on a request form that allows the approver name to be identified in print to accompany the signature. This approach also provides the opportunity to include other potentially material information like the approver’s job title or role. This provides traceability to reporting structure and supports that personnel approving the change have the authority to do so.
Lessons Learned:	Consider keeping all data and configuration in a central location to ensure SMEs can easily find baseline and configuration information. This will ensure all SMEs use the same information and information is kept up to date. This assures SMEs have the details needed to make informed decisions about when a change constitutes a deviation from the baseline and requires authorization.
Evidence:	Where a manual approach is used, consider supporting records with documented instructions that cause the requestor to generate quality records. The intention is to assure the consistent capture of enough detail identifying the relevant Cyber Assets, and how the baseline configuration is affected, as well as pertinent dates like the date of the request, the proposed

¹³ To assure compliance with baseline update obligations, and to minimize the duration that intended deviations from baselines are implemented without documented authorization, Registered Entities may want to consider a cycle with a frequency more often than the baseline update interval that must occur within 30 calendar days as prescribed by CIP-010-2 Requirement R1 Part 1.3 and the monitoring interval to detect unauthorized changes that must occur every 35 calendar days as prescribed by CIP-010-2 Requirement R2 Part 2.1.



Recommended Application Guidance – Potential Approaches (continued)

3rd Party Tool Options (continued)

Evidence: Continued	date of the change, the anticipated duration of the change, the date of the approval, and the date the change was completed, rolled back, or deferred.	
	Dated evidence of approvals for baseline change should be maintained securely as compliance evidence. If using a hard-copy manual solution with ‘wet-ink’ signatures, Registered Entities may want to consider leveraging scanning technologies to convert paper to electronic records that capture key date information to further demonstrate compliance. The below table illustrates several potential approaches to obtaining authorization manually.	
	Approval Method	Evidentiary Guidance
	Email correspondence	<ul style="list-style-type: none"> Consider supporting email approval methods with documented processes and procedures that result in the inclusion and capture of enough detail within the email identifying the pertinent Cyber Assets and how the baseline configuration is affected. Assure mechanisms are in place to appropriately classify and label emails used for baseline deviation authorizations to protect the sensitive information they are likely to contain. Consideration should be given to what protocols are necessary to protect information in transit while undergoing routing for approval. Retain the email dialogue as evidence of the approval to satisfy the documentation component of the requirement. If email archiving is used instead of saving the record to another repository, be cognizant of any retention intervals that may be configured within the email application itself and consider using shared and secured archive, so records are accessible to those who need them during audit.
	‘Wet-ink’ signature and date on a printed record	<ul style="list-style-type: none"> Consider creating a standardized change control form to help assure the details needed to demonstrate compliance are included. When a low-tech solution like this is most viable for an organization, consistency is key to minimize human performance errors. Developing tools that result in the inclusion and capture of material information like the pertinent Cyber Assets and how the baseline configuration is affected is important for quality records.
Digital signature and date on: <ul style="list-style-type: none"> A scanned record, An electronic form manually filled out and distributed electronically for approval. 	<ul style="list-style-type: none"> Consider digital signature options to capture dated approvals for manual configuration change records. This can alleviate the ‘paper shuffle’ and any need to maintain paper records. Electronic storage may also help improve indexing and evidence retrieval for audit. Consider what capabilities are available. Electronic signatures come in many forms and levels of authenticity ranging from a hand-written signature captured through a touch-screen/stylus-based device, a local self-generated and password-protected certificate, or through use of an authenticated certificate authority and individual user credentials. Consider how the signature is captured. Some approaches leverage authenticated user information (like Active Directory/LDAP) to capture the signatory name and date within the file properties or metadata in addition to the digital signature applied to the page, others can also lock the file after signing to preserve data integrity. 	



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
Exhibits:	See Exhibit L: Part 1.2. – Authorizing & Documenting Baseline Deviations (Manual Options) for a: <ul style="list-style-type: none"> • Sample Manual Configuration Change Request Form • Sample Manual Form Design Considerations
Operational Controls Samples:	1. On a cycle ¹⁴ defined by the Registered Entity, SMEs attend the Change Advisory Board meeting and provide a status update on known completed or in-flight baseline attribute changes that is compared to recently completed and open change tickets to verify that authorizations exist for deviations to baselines for the cycle. Gaps are reported to incident responders who: <ol style="list-style-type: none"> a. Investigate and resolve any conditions where approvals for intended baseline changes do not exist. SMEs complete change requests and route them for approval as documentation of the authorization. b. Investigate, report, and revert or mitigate, and document any conditions where unauthorized baseline changes are discovered.

¹⁴ To assure compliance with baseline update obligations, and to minimize the duration that intended deviations from baselines are implemented without documented authorization, Registered Entities may want to consider a cycle with a frequency more often than the baseline update interval that must occur within 30 calendar days as prescribed by CIP-010-2 Requirement R1 Part 1.3 and the monitoring interval to detect unauthorized changes that must occur every 35 calendar days as prescribed by CIP-010-2 Requirement R2 Part 2.1.



CIP-010-2, REQUIREMENT R1 – CONFIGURATION CHANGE MANAGEMENT

Analysis, Part 1.3. – Updating Baselines

Requirement Language			
CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.3	High and Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
Evaluation			
Objective:	The objective of timely updates to documented baseline configurations pursuant to Requirement R1 Part 1.3 is to assure the expected state of the baseline is known and available to support other processes that may affect the security posture, threat vectors or vulnerability status, or security assessment of a given Cyber Asset(s).		
Value Proposition:	The benefit of up-to-date baselines is that it serves as a reference point to facilitate accurate and informed decisions for security patch and vulnerability assessments, post-change security testing, detection and identification of unexpected or unauthorized changes, a basis to refer to when troubleshooting system performance or operational issues that deviate from normal, response to CIP Exceptional Circumstances or Cyber Security Incidents, and timely recovery actions.		
Recommended Application Guidance – Potential Approaches			
For each applicable Cyber Asset, after a change of a baseline configuration, the registered entity has a regulatory obligation to update the baseline configuration documentation within 30 calendar days of completing the change. Whatever approach a Registered Entity uses to achieve compliance, each organization may want to consider the importance of consistency for configuration baseline update evidence to demonstrate compliance. A potential solution is for the entity to build a process or a set of procedural instructions within their configuration change management program describing how to update the baseline configuration documentation for each type of applicable Cyber Asset and how to produce the associated dated evidence that substantiates the baseline update occurred within compliance timeframes.			



Recommended Application Guidance – Potential Approaches (continued)	
Tip:	<p>Consider testing changes prior to implementation such that baselines can be established and approved in advance and data is available once the change is completed. While not required, this approach can help lessen the burden of tracking a 30-calendar day clock for individual changes, can serve to inform the SME to support the pre-change security impact assessment, and can provide additional assurance that compliance documentation of the anticipated post-change baseline is generated well within the required timeframe. It should also be noted that CIP-007-6 Requirement R1 Part 1.1 causes Registered Entities to document the need for enabled logical network accessible ports (inclusive of ranges or services where needed to handle dynamic ports) and this obligation does not include a 30-calendar day timeframe. CIP-007-6 R1.1 does not require Registered Entities to document the need for enabled logical network accessible ports prior to the enabling of said ports. CIP-007-6 R1.1 requires Registered Entities to enable only logical network accessible ports that have been determined to be needed by the Registered Entity. An entity that has enabled only those logical network accessible ports that have been determined to be needed has met this requirement regardless of when their documentation was created.</p> <p>As a result, Registered Entities who use the CIP-010-2 configuration baseline as the sole documentation for the determination of need must recognize that because CIP-007-6 R1.1 does not include a 30-calendar day timeframe; if a change enables logical network accessible ports that are not needed and the Registered Entity fails to take the actions necessary to disable the port on the day the change was implemented (and thus, the day the port was enabled) then the Registered Entity may be in violation of CIP-007-6 R1.1 and this may not be caught until the Registered Entity takes the actions necessary to review and update their baseline configuration per CIP-010-2 R1.3.</p>
Lessons Learned:	<p>Consider documenting what constitutes the completion of a change to set clear expectations for affected SMEs on when the 30-calendar day compliance timeframe for baseline updates begins and ends. For any process, clear expectations help reduce human performance errors and help inform users of the process on what actions must be taken and when.</p>
Evidence:	<p>A dated version of the baseline should be retained as evidence inclusive of the date each attribute was modified to demonstrate the baseline update was completed within 30 calendar days of the change to the attribute(s).</p> <p>Consider the inclusion of supporting evidence, which may include:</p> <ul style="list-style-type: none"> • Change records that demonstrate the baseline change was approved and executed in accordance with the entity's configuration change management process. • <i>System-generated</i> evidence from the Cyber Asset demonstrating the actual state of the attribute configuration. • A manual or automated configuration change management process should be provided to support how evidence is generated. Also, the change request and approval for each baseline configuration change should be retained, with corresponding <i>system-generated</i> evidence attached to, or otherwise stored with, each change request. • The entity may consider performing its CIP-009 system recovery procedure to update the backup image that reflects the baseline configuration changes as the baseline configuration changes may affect the Cyber Asset recovery.



Recommended Application Guidance – Potential Approaches (continued)	
Operational Controls Samples:	<ul style="list-style-type: none"> • On a cycle defined by the Registered Entity, the responsible party creates a calendar event within an email system or other office productivity tool and configures it to remind/alert on the impending 30 calendar day due date within a specified interval before the deadline. • On a cycle defined by the Registered Entity, the work management system will automatically send alerts through the configured alerting mechanisms to the responsible party of any impending 30 calendar day due date. • The granularity and rigor of a Registered Entity’s process(es) will typically dictate how an alert reference is configured. For Example: <ul style="list-style-type: none"> ○ Alert Trigger/Cycle: Alerts could be configured to start at a preset number of days prior to the due date. Alerts could also be based on the approval for the work or an actual step within the work process. • Alert Mechanism: Depending on the available options, alerts could be set to email a person or group. Alerts could also be set up to appear in a monitoring display or task queue. Alerting might also be accomplished by setting a flag in a system that triggers inclusion in a view, dashboard, or report that is manually reviewed and acted upon to inform the responsible party.
3rd Party Tool Options	
<p>Most 3rd Party Tools update baseline information as a part of the core functionality of the tool when variances are detected. Some tools also provide accept, reject, or acknowledgement features that can be used to serve as an additional means to demonstrate the new baseline was reviewed for accuracy and completeness before making it official.</p> <p>It is important to retain the <i>system-generated</i> historical changes including the completion date of each baseline configuration change and the completion date of each baseline configuration documentation update following the change. These two <i>system-generated</i> completion dates are used to prove the registered entity has updated its baseline configuration documentation within the required time window.</p>	
Tip 1:	Auto discovery and acknowledgement features can bring operational efficiency to the process, standardize response to detected changes, while also serving to collect timestamped evidence needed to demonstrate compliance with CIP-010-2 Requirement R1 Part 1.3.
Tip 2:	Out of the Box (OOB) capabilities and configurable features are different than customization. Insisting the vendor make this distinction and demonstrate OOB capability can save Registered Entities significant time and resources and assure the 3rd Party Tools can meet the need.
Lessons Learned 1:	SMEs have a lot of dates and cycles to manage and remember. When using a 3rd Party Tool, leveraging the system by including a field for a due date, and configuring the system to generate reminders can help set SMEs up for success for updating the baseline documentation within 30 calendar days. See the Tip in the main section of Part 1.3 for a caution about documenting determination of need for logical network accessible ports.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Lessons Learned 2:	<p>Registered Entities should be cautious of overreliance on technology to serve as a sole and single source of all records and may want to consider alternative approaches to how success can be achieved under conditions where the 3rd Party Tool may be unavailable.</p> <p>Additionally, while specific to security patching, Lessons Learned 2 from the 3rd Party Tools Section for 1.1.5 illustrates another potential type unintended consequence and alternatives to prevent these types of conditions that Registered Entities may want to consider if using a 3rd Party Tool to house all baseline records.</p>
Evidence:	<p>3rd Party Tools configured to monitor systems can also be configured to automatically gather (R1.1.1) OS/FW version (R1.1.2 – 1.1.3) open source, commercially available, and custom software installed including version where applicable, (1.1.4) network accessible logical ports, and (1.1.5) applied security patches and retain as evidence.</p> <p>Evidence could include on-demand reports generated by the 3rd Party Tool, or extract/exports from the database or its logs of detected events or alerts.</p> <p>Supporting evidence may also include date and timestamped point-in-time snapshots from the 3rd Party Tool that the Registered Entity has extracted from the system and retained with other artifacts such as change tickets, approvals records, or testing results.</p> <p>Supporting records may come direct from a Cyber Asset in the form of <i>system-generated</i> evidence.</p>
Operational Controls Samples:	<p>Through the configuration of the 3rd Party Tool, and on a cycle defined by the Registered Entity, the 3rd Party Tool will continue to alert on detected changes until the update to the baseline attribute(s) is acknowledged.</p>
Manual Options	
<p>After a baseline change is completed the baseline attributes in your manual tracking repository (which could be a spreadsheet or database) must be updated within 30 calendar days to meet the compliance obligation. It is ideal to do this immediately following the change, so it is not overlooked in a manual process. Manual systems tend not to have alerting systems for time requirements and can be prone to missing time requirements. It is also important to make sure the baseline attributes track the date of the change completion and updated date of the baseline in demonstration of compliance.</p>	
Tip:	<p>Consider storing all information required for evidence in a central authoritative location so SMEs can quickly and accurately find information for baseline comparison. Utilizing an existing asset management or protection system settings system for baseline history prevents having to maintain devices and baseline attributes in multiple locations. See the Tip in the main section of Part 1.3 for a caution about documenting determination of need for logical network accessible ports.</p>



Recommended Application Guidance – Potential Approaches (continued)

Manual Options (continued)	
Lessons Learned:	Registered Entities may want to consider having a date field or revision table within the database or document itself where the date can be manually recorded. Solutions that include the content of the record in concert with the technical versioning control of a system can help demonstrate compliance. It can also serve to reconcile unintended or unexpected discrepancies when looking back on records or providing them for regulatory oversight activities.
Evidence:	<p>Where Cyber Assets are capable of producing dated <i>system-generated</i> records, entities may want to consider using this evidence to demonstrate compliance for Requirement 1.3 as <i>system-generated</i> time/date stamps can be difficult to falsify and may be more reliable. For the date of completing a baseline configuration change, where a Cyber Asset can produce dated <i>system-generated</i> baseline information the evidence could be a system log, system report, or screenshot etc. As long as it is <i>system-generated</i>, includes the date and time, and some unique attribute traceable to the Cyber Asset, the record could be stored in the system and retrieved upon request, or could be exported and stored in a secure repository. Note that the Registered Entity only needs to retain the <i>system-generated</i> completion date for a finalized change as an applied change may be rolled back, provided that the change caused an adverse impact to operations or the required cyber security controls in CIP-005 and CIP-007. For example:</p> <ul style="list-style-type: none"> • Example 1: For a newly installed security patch on an operating system based Cyber Asset, a .csv file can be exported from Control Panel - Security Update under Programs and Features to demonstrate the security patch ID and the installation date. • Example 2: For a firmware update on an IED, a screenshot can be used to demonstrate the updated firmware version and the installation date. <p>For the date of completing a baseline configuration documentation update, consider storing the evidence in a document management system or an asset management system with a <i>system-generated</i> version history including date and time. This <i>system-generated</i> configuration documentation update date compared to the change completion date demonstrates the update was made within 30 calendar days of completing the change. For example:</p> <ul style="list-style-type: none"> • Example 1: Where manual paper-based solutions are used; manual recording of dates and version on a baseline record could be an option. It could be in hardcopy format or stored electronically after scanning. Consider recording a change request number on the record for traceability. • Example 2: If a document management system with automated versioning history is used for managing the baseline configuration, the baseline documentation version history that is generated by the system can be used to demonstrate the baseline documentation version and the date of completing the update. Consider recording a change request number in the version history comments field so that it would be used to track which changes are reflected in this baseline documentation version. Entities could also designate a field in the system for the manual entry of the date baseline updates were completed.



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
	<ul style="list-style-type: none"> Example 3: If an asset management system is used for managing the baseline configuration items, <i>system-generated</i> change history including the version and the date of completing the update could be retained as evidence.
Exhibits:	See Exhibit M: Part 1.3. – Updating Baselines (Manual Options) for an example relay setting report that depicts a manually updated baseline configuration.
Operational Controls Samples:	<ol style="list-style-type: none"> Occasionally spot-checking steps in the change management records to ensure proper requests and baseline updates are made. Note: if performing this check within 30 calendar days of the completion of an approved baseline change, it serves as a preventative control. If performing this check after the completion of an approved baseline change it serves as a detective control. See Operational Controls Samples for Part 2.1 Manual Options.



CIP-010-2, REQUIREMENT R1 – CONFIGURATION CHANGE MANAGEMENT

Analysis, Part 1.4. – Assessing and Testing Cyber Security Controls

Requirement Language			
CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.4	High and Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Evaluation			
Objective:	The objective of pre-change security impact assessment, post-change security testing, and documentation of security testing results pursuant to Requirement R1 Part 1.4 is to assure baseline configurations changes that obviate implemented security controls are identified and remediated. This helps assure the security posture of a given Cyber Asset(s) is maintained and security controls continue to operate as designed. Below are several potential approaches to accomplishing this objective.		
Value Proposition:	<p>A benefit of having established configuration baselines is the knowledge and awareness it brings to 1) the known and expected state, 2) the necessary operational settings/parameters, and 3) the security design and posture of a given Cyber Asset, at either the individual host level or for a given category of infrastructure.</p> <p>Changes that affect attributes of established baselines for any Cyber Asset come with some level of risk. Whether the change is intended to 1) adjust functionality or feature sets, 2) address a security vulnerability, and/or 3) fix an operational performance issue or bug; implementing changes has the potential to introduce unknowns or unexpected/unintended results that could obviate otherwise effectively designed and operational security controls.</p> <p>Knowing the expected configuration baseline of a Cyber Asset is an important first step in assessing and mitigating this risk. Effectively monitoring, managing, and approving changes to established baselines is just as important</p>		



Recommended Application Guidance – Potential Approaches

Where applicable BES Cyber Systems (BCSs) and associated Cyber Assets are concerned, changes to established baseline may pose risk to the security and operability of BES Cyber Systems that support reliability of the Bulk Electric System (BES). CIP-010-2 Requirement 1 Part 1.4 prescribes a set of controls to help prevent and/or detect unauthorized baseline changes BCSs. This approach causes Registered Entities to control configuration changes in a manner that supports protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

CIP-010-2 Requirement 1 Part 1.4, calls for Registered Entities to perform a security assessment inclusive of specified components when performing changes that deviate from existing baseline configuration.

In analyzing this requirement part, these components include:

1. Pre-change determination of potential impacts to required cybersecurity controls in CIP-005 and CIP-007,
2. Post-change verification that cybersecurity controls in CIP-005 and CIP-007 continue to be implemented and operating as designed, and
3. Documented results that demonstrate the verification was performed.

One approach a Registered Entity might consider is to perform an analysis of CIP-005 and CIP-007 to derive a list of the required cybersecurity controls that may serve as a basis for the pre-change impact determination. The output of this pre-change assessment may then serve to scope or define the post-change verification and documentation that is required.

One potential approach to establishing a list of required cybersecurity controls could be to list them out at a high level for CIP-005 and CIP-007 and incorporate this into a single Standard Operating Procedure that serves cross-functionally within an organization. Refer to [Appendix D](#) for supporting analysis and tools.

If departmental infrastructure or practices are too diverse to centralize an approach, another potential option could be for a Registered Entity to begin with a high-level list and extrapolate it out based on relevant factors or Functional Area needs.

Others may decide to align across the organization with a standardized/centralized definition of what a pre-security impact assessment and post change testing should include and then allow each affected Functional Area to determine how best to execute under those parameters.

Whatever the approach, consistency and repeatability is a sound consideration for any Registered Entity. Being aligned as an organization can help bring efficiencies to the process, consistency to the records, and help the Registered Entity avoid common mistakes or gaps. The sections to follow detail 3rd Party Tools based and Manual options for which a hybrid solution could be derived by implementing various ideas in whatever combination is most preferable by the Registered Entity.

Tip 1:	If choosing to conduct a CIP-005 and CIP-007 analysis for deriving a list of security controls, some other important things to consider may be how Cyber Assets are interconnected, if there are downstream hosts, applications, systems, or support personnel that might be involved in end-to-end operability of security controls, and what cross functional dependencies may affect the process for assessing security risk.
---------------	--



Recommended Application Guidance – Potential Approaches (continued)	
Tip 2:	<p>Because no two Registered Entities are alike, each organization may want to consider other factors that could impact the chosen approach. A Registered Entity’s structure, resources, skill sets, and tool sets may lend better to one approach than another. Additionally, the architecture and individual Cyber Asset function may also influence which attributes are relevant to pre-impact assessment, a given Functional Area, or a category of Cyber Asset.</p> <p>For a Registered Entity’s applicable BES Cyber Asset(s)/System(s) and/or associated Cyber Asset(s), some examples of factors that might influence a Registered Entity’s approach could be, and may not be limited to:</p> <ul style="list-style-type: none"> • Cyber Asset infrastructure category or type(s), • Logical environment and/or connectivity characteristics, • Technical capabilities/characteristics that may be unique or specific, • Staff resources, knowledge base, and/or support structure/service level agreements, • Frequency, volume, duration, or complexity of change • Change type (add/change/remove), • Change category or Framework/Model/Practices used (e.g. standard/normal/emergency1), • Cross functional relationships and/or dependencies, • Cultural maturity from a security and compliance perspective, or • Supporting technologies that may offer process consistency, efficiency, repeatability, and/or automation.
Lessons Learned 1:	<p>Registered Entities may want to consider the level of detail, complexity, ease of use, and potential administrative components of any given option. A perfectly defined and/or technically controlled/prescriptive solution may not reap intended benefit if it is so burdensome to use that no one does. Sometimes keeping it simple can improve the chance for success.</p> <ul style="list-style-type: none"> • Consideration of the inputs and the outcomes (resource investment vs security objective) may help to right size the solution and strike the balance between rigor and ease of use. This may also help Registered Entities avoid analysis paralysis and solutions that may be of diminishing returns. • Human performance factors may be another consideration and having a holistic and comprehensive understanding of the end user base of the processes or tools, their job function, and their skill sets. Aligning tasks with skills and recognizing the risks associated to human performance can be a critical element to the success in implementing solutions for this part of the requirement. Having the right resources with the right skills performing the pre-change assessment could prevent the introduction of security gaps. • Another consideration Registered Entities may want to make is what level of flexibility is appropriate to have within the process, and to define where deference to Subject Matter Expertise is permitted or necessary. Sometimes the most prescriptive or well-defined approach can have the unintended consequence of removing discretion when it may be needed most. • Keeping the objective of security and reliability as a key consideration may help Registered Entities avoid common mistakes that could lead to unnecessarily administratively burdensome compliance-focused solutions that distract from security objectives or risk reliability.



Recommended Application Guidance – Potential Approaches (continued)**Lessons Learned 2:**

Certain systems may have dependencies on a Cyber Asset(s) other than the one undergoing the baseline configuration change that could impact the operability of cybersecurity controls. Being cognizant of the interoperability between systems can prevent unintended consequences. Consider the following scenario (Note: Evidence listed is not prescriptive and serves as one example of one potential way to perform/evidence a verification process):

A server undergoes an authorized baseline configuration change to upgrade to a new version of the Windows Operating System. During the pre-security impact assessment, the SME identifies that logging and alerting controls for security events may be impacted. The SME performs the change and begins the post-change impact assessment. As a part of the procedure to verify the logging and alerting controls for security events:

1. The SME reviews the Windows settings and verifies the setting to enable successful and failed login attempts within the Security Event log are checked. A screenshot is taken as supporting evidence and 'pass' is recorded in the test results.
2. The SME then verifies the server's interface and default gateway configuration, and confirms the server is also configured to send the Security Event log to a centralized server by checking that the syslog receiver IP address is that of the centralized system. A screenshot is taken as supporting evidence and 'pass' is recorded in the test results.
3. Next, the SME generates a successful login and an intentional failed login and views the local log file as well as the centralized log server to confirm the entries. Both systems contain the events. A screenshot is taken as supporting evidence and a 'pass' is recorded in the test results.
4. The SME intentionally fails 5 consecutive logins to test account disablement thresholds and alerting mechanisms. On the sixth attempt the SME enters valid credentials and receives an error that the account has been locked. A screenshot is taken as supporting evidence and a 'pass' is recorded in the test results.
5. The SME is also an administrator of the server and is waiting for the alert that the threshold for failed logins has been exceeded and the account was locked. The SME waits and after 5 minutes the alert is not received. A 'fail' is recorded in the test results and the SME begins investigating.
 - a. Upon troubleshooting the SME learns that the Upgrade from one Windows Server version to another changed the order that data is stored in the event logs and the centralized server was monitoring the wrong field for failed logins. The SME identified the correct field by reviewing which column had incremented to 5.
 - b. The change management process is used to modify the centralized server's configuration to monitor the correct field for Security Event logs from Windows servers with the new Operating System version. These mitigating actions are recorded in the test results.
 - c. The test is reperformed and the alert was received. A 'pass' is recorded in the test results.
6. Once all security control testing activities are performed and the security posture is verified, the change is marked complete and the baseline is updated within 30 calendar days.



Recommended Application Guidance – Potential Approaches (continued)	
Lessons Learned 2: (continued)	<p>7. As a best practice, the Registered Entity has a corrective actions and continuous improvement program that includes a post implementation review (PIR) of any change that contained a ‘failed’ security test result. This PIR occurs on a cycle defined by the Registered Entity and includes documented Lessons Learned. From this scenario, actions to update testing and recovery procedures were performed to assure the centralized logging server is included in change requests to upgrade the Operating System of Cyber Assets.</p>
Evidence:	<p>Whether generated from a 3rd Party Tool or captured through execution of a manual process(es), recommended evidence to retain could include, and is not limited to:</p> <ul style="list-style-type: none"> • Dated change request records that uniquely identify the Cyber Assets (or group of Cyber Assets with traceability to each unique device) and a description of the baseline deviation that will occur, inclusive of the authorization records to make the change. • Dated records including the CIP-005 and CIP-007 cybersecurity controls considered as a part of the pre-change security impact assessment, as well as each determination of potential impact for each evaluated control, assuring the completion date is prior to the planned or actual implementation date of the actual change request. • Dated records to document the performance of post-change verification that cybersecurity controls in CIP-005 and CIP-007 continue to be implemented and operating as designed, assuring the completion date on these records is after the change to baseline configuration changes. • Dated records documenting any post-change verification conclusions where unanticipated impacts occurred, the response and mitigating actions to address adverse results (or evidence the Cyber Asset or System was rolled back) demonstrating a secure and compliant end state. <p>Registered Entities should also consider capturing supplemental evidence to demonstrate compliance.</p> <ul style="list-style-type: none"> • Supplemental records in the form of <i>system-generated</i> evidence of before and after baseline configuration can help demonstrate compliance and can also satisfy the requirement to update baselines within 30 calendar days as prescribed by CIP-010-2 Requirement R1 Part 1.3. • Dated reports, exports, logs, or other relevant outputs of commands or tools from the Cyber Asset(s) that underwent change, or from related Cyber Assets used to perform the CIP-005 and CIP-007 cybersecurity control demonstrating the actual operational state of the control is in alignment with the results documented within the post-change security posture verification records. <p>Lessons Learned 2 from this section serves as an example of a test procedure where supporting evidence may come from a Cyber Asset other than the one undergoing the baseline configuration change. Consider the following scenario (Note: Evidence listed is not prescribed by the standard and serves as an example of one potential way to perform a verification process):</p>



Recommended Application Guidance – Potential Approaches (continued)	
Operational Controls Samples:	<ol style="list-style-type: none"> 1. Upon the authorization of the request to change baseline configuration, using the form within the change management system (or using a checklist) containing CIP-005 and CIP-007 security controls), the responsible SME evaluates the potential impact the baseline change poses to Cyber Asset security posture and documents the results. 2. Upon completion of a pre-change security impact assessment, the responsible SME provides the documented conclusions to a team member for peer review and comments. Comments of the peer are considered prior to the implementation of baseline configuration changes. 3. Upon the implementation of baseline configuration changes and using the documented results of the pre-change impact assessment, the SME refers to procedures to execute tests for each CIP-005 and CIP-007 security control identified as having a potential impact. Where it is verified that cybersecurity controls in CIP-005 and CIP-007 continue to be implemented and operating as designed the SME documents the results and captures dated evidence that support each conclusion. Where unanticipated results are identified, the SME documents the results, investigates the condition, and in accordance with change control processes: <ol style="list-style-type: none"> a. Executes actions to restore affected security controls, b. Implements compensating measures to mitigate the issue, c. Or rolls back the baseline configuration change
3rd Party Tool Options	
As one approach, a Registered Entity with mature centralized Change Control and Configuration Management tools may choose to integrate the pre-change security impact assessment and the post change security testing into an automated workflow within available implemented tools sets.	
Tip 1:	Consider incorporating provisions for emergency changes such that restoration of security and reliable operations may be prioritized and addressed unencumbered by administrative tasks associated to formal change control and without compromising the determination of potential impacts to required cybersecurity controls in CIP-005 and CIP-007. One potential approach could be utilizing 3rd Party Tools for the performance of the security impact assessment contemporaneously with emergency response actions.
Tip 2:	Although a CIP Exceptional Circumstances (CEC) cannot be taken for compliance with Part 1.2, the criterion in the CEC definition may provide a starting point for when use of the emergency change process is acceptable.
Lessons Learned:	Registered Entities may want to consider defining what constitutes an emergency change, leveraging in-system workflow capability to assure relevant routing and priority of emergency changes, in addition to documenting and implementing monitoring and governance practices that provide reasonable assurance that emergency change processes are not used as a workaround to pre-planning for change.
Evidence:	<ul style="list-style-type: none"> • <i>System-generated</i>, dated, and timestamped exports or screenshots of baseline configuration change records from the 3rd Party Tools used to request, assess, authorize, and execute changes. Records should uniquely identify the Cyber Assets (or group of Cyber Assets with traceability to each unique device) and a description of the baseline deviation that will occur, inclusive of the authorization records to make the change.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Evidence: (continued)	<ul style="list-style-type: none"> • Approved versions of methodologies and/or design specifications that identify any criteria and/or programmatic logic of any 3rd Party Tool configuration where technology is used to systematically identify which CIP-005 and CIP-007. • Approved versions of departmental operating procedures used to pre-change security assessments, post-change security controls validation, and associated completed records/exports from the 3rd Party Tool documenting the execution of procedures. • System-generated, dated, and timestamped exports or reports from 3rd Party Tools used to assess CIP-005 and CIP-007 records including the CIP-005 and CIP-007 cybersecurity controls considered as a part of the pre-change security impact assessment, as well as each determination of potential impact for each evaluated control, assuring the completion date on these records is prior to the planned or actual implementation date of the actual change request. • System-generated, dated, and timestamped reports from 3rd Party Tools used to detect baseline changes and automate the comparison for post-change verification of security posture. • Dated SME assessment records to document the outcome of post-change verification that cybersecurity controls in CIP-005 and CIP-007 continue to be implemented and operating as designed, assuring the completion date on these records is after the change to baseline configuration changes. • Dated records documenting any post-change verification conclusions where unanticipated impacts occurred, the response and mitigating actions to address adverse results (or evidence the Cyber Asset or System was rolled back) demonstrating a secure and compliant end state. <p>Also refer to the parent Evidence Section of Part 1.4 for additional evidence suggestions.</p>
Exhibits:	See Exhibit N: Part 1.4. – Assessing and Testing Cyber Security Controls (3rd Party Tool Options) for an example of an export from a change management system configured to technically control that a security questionnaire is completed based on change type and per Cyber Asset capability.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. During the design phase for the implementation of a 3rd Party Tool to support the change management process, the design team, in coordination with SMEs responsible for managing Cyber Assets subject to CIP-010-2 obligations, defines Cyber Asset profiles and which include security capabilities relevant to CIP-005 and CIP-007. 2. During the design phase for the implementation of a 3rd Party Tool to support the change management process, the application development team, in coordination with SMEs responsible for managing Cyber Assets subject to CIP-010-2 obligations, develops a pre-security assessment methodology and post-testing criteria that leverages Cyber Asset profiles so programmatic intelligence can be built into the system to identify which security controls must be tested for certain types of Cyber Assets and baseline changes. This logic is built into a survey within the system that is driven by workflow configured in the tool.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
<p>Operational Controls Samples:</p> <p>Continued</p>	<ol style="list-style-type: none"> 3. Per the occurrence of an approved change to baseline, the SME completes a survey in the 3rd Party change management system which applies programmatic logic to automatically identify which security controls in CIP-005 and/or CIP-007 could be impacted by the change. Where controls are managed by another functional area the system identifies the dependency from the relational database information and automatically includes the relevant SME contact(s) needed to perform post-change security testing to coordinate the change with that group(s). 4. Upon the detection of baseline changes, the 3rd Party Tool monitoring change executes an automated process(es) to perform credentialed security scans and collect relevant CIP-005 and CIP-007 Cyber Asset information. The system performs a comparison of this data to the most previous known state and stores a variance report to support post-changes security posture evaluation by the SME. The variance report identifies the two source reports from the Cyber Asset used for comparison.
Manual Options	
<p>Using a job aid like a standardized checklist for pre- and post-implementation is one approach that can help ensure all potential impacts to CIP-005 and CIP-007 security controls are evaluated and verified. The checklist can also provide documentation and evidence of evaluating and verifying security controls to demonstrate performance of CIP-010-2 R1 Part 1.4.</p> <p>Another Registered Entity may find that a manual or paper-based solution is more affordable or practical for the level of change and the pace of their organization.</p> <p>To ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely impacted by authorized baseline configuration changes they should be incorporated into the baseline configuration change management system.</p> <ol style="list-style-type: none"> 1. Each required cyber security control from CIP-005 and CIP-007 should be identified. 2. To ensure only the relevant cyber security controls are verified with a given baseline change, all possible baseline configuration change types should be defined. 3. Each type of baseline configuration change should be cross-referenced with the required cyber security controls and the relevant controls identified. 4. The defined baseline configuration change types should be incorporated into the change management system. 5. Each change ticket should require that the relevant cyber security controls are verified before the change request can be closed. <p>To help ensure cyber security controls are verified locally on the device immediately after the baseline configuration change is made, consider expecting specific checks be added to the change request. These checks are based on the make and type of device, such as a specific brand or model of relay or RTU and describe exactly what to verify on the device. If the change request is issued as a paper copy, the completed paper change request form should be scanned and saved with the change request in the change management system or repository to document exactly what was done to verify the cyber security controls were not adversely impacted.</p>	



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
Tip 1:	Consider including steps for the capture of evidence within the procedure and/or checklist/security testing forms/tool so that clear expectations are set for personnel performing the change. This can reduce human performance errors, prevent rework, and improve the consistency and quality of records needed to demonstrate compliance.
Tip 2:	Testing after a change is performed to assure security posture. Even with the best planning, it is reasonable to expect that unanticipated conditions could result from change. Instead of troubleshooting and fixing these conditions to mark testing complete, assure SMEs recognize the value in documenting unexpected conditions and the actions needed to resolve. This provides the opportunity to discuss lessons learned and update instructions for the next SME to prevent those conditions going forward, while fostering a culture of transparency, security, and continuous improvement.
Lessons Learned 1:	If Cyber Assets undergoing change leverage other Cyber Assets or Systems, to accomplish CIP-005 and/or CIP-007 security controls, assure personnel performing the change: have lined up other relevant functional areas(s) for any needed coordinated testing/evidence collection.
Lessons Learned 2:	<p>If Cyber Assets undergoing change do not have External Routable Connectivity and Interactive Remote Access capability through an Intermediate system, assure personnel performing the change are:</p> <ul style="list-style-type: none"> • Equipped with all the necessary tools and access authorizations to perform the identified security tests or other SMEs who may be needed to do so. • Versed in the policies and appropriate use of Transient Cyber Assets and/or Removable Media where needed to capture evidence. <p>This can increase efficiency and help prevent undue delay, incomplete testing, and/or extra site visits to complete the tasks.</p>
Lessons Learned 3:	Registered Entities may want to consider defining what constitutes an emergency change, in addition to documenting and implementing associated manual monitoring and governance practices that provide reasonable assurance that emergency change processes are not used as a workaround to pre-planning for change.
Evidence:	<ul style="list-style-type: none"> • Dated and approved Change Request records. • Dated manually generated records of: <ul style="list-style-type: none"> ○ Approved pre-change baseline configuration of the applicable production Cyber Asset. ○ Dated documents that cross-reference baseline configuration change with the required cyber security controls and the relevant controls identified for testing. ○ Records documenting the status of tested security controls and the pass/fail results of overall testing, inclusive of any actions to address identified issues. ○ Post-change security controls testing results ○ Post-change baseline configuration of the production Cyber Asset • Also refer to the parent Evidence Section of Part 1.4 for additional guidance.



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
Exhibits:	See Exhibit O: Part 1.4. – Assessing and Testing Cyber Security Controls (Manual Options) for an example of a mechanism to capture a manual security assessment and testing record.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. Per the occurrence of an approved change to baseline, the SME completes a checklist to identify which security controls in CIP-005 and/or CIP-007 could be impacted by the change. Where controls are managed by another functional area the SME coordinates the change with that group(s). 2. Upon the execution of an approved change to baseline configuration, using the pre-security impact assessment checklist, the SME(s) performs testing to verify identified security controls for CIP-005 are implemented and operating as designed. Variances are documented and investigated until security posture is restored. Actions to restore security posture are documented and provided for post implementation review processes. 3. See also parent Operational Control Samples for Requirement R1 Part 1.4 for more ideas.



CIP-010-2, REQUIREMENT R1 – CONFIGURATION CHANGE MANAGEMENT

Analysis, Part 1.5. – Testing High Impact Baseline Changes

Requirement Language			
CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber	<p>Where technically feasible, for each change that deviates from the existing baseline configuration:</p> <p>1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and</p> <p>1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.</p>
Evaluation			
Objective:	<p>The objective of pre-change testing, documented differences between test and production environments (where a test environment is used), and documented testing results pursuant to Requirement R1 Part 1.5 is to assure baseline configuration changes minimize the risk of adverse impact to production operations. Pre-change testing helps provide reasonable assurance that post-change security posture of a given Cyber Asset(s) is known prior to implementation.</p>		
Value Proposition:	<p>Pre-change testing can discover unexpected results from baseline changes. This offers the opportunity to test and verify that CIP-005 and CIP-007 security controls are operating as designed, to assess security risk and adverse impacts were controls are not operating as expected, and to implement compensating or mitigating measures for any identified vulnerabilities that may be introduced from features that are not needed or unintended consequences of the baseline configuration change. This visibility allows the SME to identify and document the steps needed to stabilize the configuration to a known secure state before introduction into an operating environment. An understanding of the potential impact to the system and users helps assure informed decisions relative to the timing and duration of the production change, allows for planning and testing of the steps to perform when</p>		



Evaluation (continued)	
<p>Value Proposition: (continued)</p>	<p>implementing in production, minimizes the likelihood that the change will be disruptive or require rollback, and minimizes the risk of human performance errors that can manifest from performing baseline changes in an uncontrolled manner. These benefits in combination minimizes risk to safe, secure, resilient, and reliable operation of the BES.</p>
Recommended Application Guidance – Potential Approaches	
<p>CIP-010-2 Requirement R1 Part 1.5 consists of two components, testing baseline changes for high impact BES Cyber Systems and documenting the results and the characteristics of any test environment and testing measures used. To the extent possible, pre-change testing should be done in an environment that models the baseline configuration to ensure that required cyber security controls are not adversely affected. The results of the security controls testing should be documented for evidence.</p> <p>Registered Entities may want to consider investing in a test environment that models the high impact BES Cyber System so needed changes that deviate from existing baselines can be thoroughly tested and planned before being performed on a production system.</p> <ul style="list-style-type: none"> • When implementing a test environment, consider what infrastructure is needed to reasonably simulate the production environment. It is not necessary to replicate the infrastructure one-for-one; however, it stands to reason that the more closely the hardware, software, topology, and redundancy mirrors production, the more realistic the test scenarios can be, and the more representative and accurate the test results should be. A test environment that closely mimics production can provide better assurance that security or operational issues will be discovered before they can adversely impact operations. • The ability to detect and assess adverse results in a test environment and determine how to mitigate or resolve them ahead of time can improve the chances of the baseline change being successfully and seamlessly implemented in a secure and controlled manner when performing it in production. • Testing changes before implementation in production also provides the opportunity to pre-define the future expected baseline. Having an anticipated updated baseline can aid the SME in confirming expected results when implementing later in production. • Identifying and documenting variances between test and production systems can help SMEs be efficient in testing and prepare personnel for what tests will produce the most effective and accurate results, and what additional measure may need to be taken to accommodate for differences when promoting to production. <p>If a test environment is not available, Registered Entities can still employ techniques and cautionary measures to minimize the potential adverse effects a baseline change can have on production. It is recommended that Registered Entities consider these precautionary measures, in combination to help reduce the risk that production changes to baseline can pose to the system when a test environment is not an option.</p> <ul style="list-style-type: none"> • While it is recommended that SMEs educate themselves on the potential impacts of any baseline change, when performing a change in production it becomes more critical. It is recommended that SMEs thoroughly review any vendor materials that are available for the type of baseline change being performed. It is common for vendors to publish release notes for new major or minor versions of operating systems, firmware, commercially available application software, and package updates, security 	



Recommended Application Guidance – Potential Approaches (continued)

patches, hot fixes, or feature enhancements. These release notes can offer great insight into details like, but not limited to, backwards compatibility issues, fixes that may be intended to solve operational issues or mitigate security vulnerabilities, feature enhancements that may alter needed services and open ports, and/or default settings or new accounts that may be introduced upon implementation that could negate intended security controls.

- Assuring changes are well communicated to end users can also prove fruitful because system users are typically intimate with the normal operations of the high impact BES Cyber System and may have the ability to more quickly detect if anything is not operating as expected
- Scheduling the change for a time that coincides with non-peak periods and where the use or strain on the system is less can help minimize operational impacts.
- Taking the precaution of lining up additional SMEs to assure expertise is available if the change causes unintended operational impacts is recommended.
- When having to impact directly in production, having a plan to rollback or isolate the Cyber Asset may also be a prudent measure.
- Where redundantly configured Cyber Assets exist, performing the change on one Cyber Asset as a test and allowing it to operate in the environment for a predefined period before applying it to other like systems can provide the opportunity to discover and address unintended configurations that create security gaps or operational issues. Also, where the high impact BES Cyber System environment contains PCAs and BCAs that are similarly configured, implementing the baseline change on the less critical Cyber Asset first can afford the SME the opportunity to identify any risks or issues before the change is performed on a BCA.

3rd Party Tool Options

The same 3rd Party Tools that can be implemented to achieve and maintain compliance with CIP-010-2 Requirements R1 Part 1.1 – 1.4 can be used to assist a Registered Entity with achieving compliance with the testing requirements of Part 1.5.

- Consider purchasing licensing that will allow for a secondary instance of tools within a test environment.
- Designing and implementing a process to export copies of approved production baselines from the production baseline monitoring tool or repository so they may be imported or loaded into the tool used in test. This can serve as the basis to confirm that the test system undergoing change is starting with a configuration that truly models the baseline of production. It may also help automate the process to detect baseline variances and unanticipated results during testing. Capturing dated inputs and outputs of the tool before, during, and after testing can accomplish the required documentation of variances between test and production environments needed to demonstrate compliance with Part 1.5.2.

Tip 1:	The 3rd Party Tool could generate a survey or questionnaire to ensure the SME doesn't forget to answer any question or forget any testing steps.
Tip 2:	The 3rd Party Tool could automatically gather baseline information and notify SME of any changes. The SME would then validate if the changes were planned or not.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Tip 3:	Consider incorporating provisions for emergency changes such that restoration of security and reliable operations may be prioritized and addressed unencumbered by administrative burdens and without compromising the ability to pre-test and minimize potential adverse impact to production environments. One potential approach could be utilizing 3rd Party Tools for the performance of the security testing contemporaneously with emergency response actions.
Tip 4:	Although a CIP Exceptional Circumstances (CEC) cannot be taken for compliance with Part 1.5, the criterion in the CEC definition may provide a starting point for when use of the emergency change process is acceptable.
Lessons Learned 1:	The 3rd Party Tool should be easy to use to minimize SME mistakes when entering data and comparing baselines.
Lessons Learned 2:	Data in the 3rd Party Tool should be validated periodically to ensure accuracy.
Lessons Learned 3:	Registered Entities may want to consider defining what constitutes an emergency change, in addition to documenting and implemented monitoring and governance practices that provide reasonable assurance that emergency change processes are not used as a workaround to pre-planning for change and performing the pre-testing required by Requirement R1 Part 1.5.
Evidence:	<p>An approved Change Request; inclusive of pre-cautionary measures taken if a test environment is not used, the CIP-005 & CIP-007 cyber security controls that may be impacted by the change, and the state each control is expected have upon completion of the change. Registered Entities should also consider capturing and retaining dated and timestamped <i>system-generated</i> evidence of:</p> <ul style="list-style-type: none"> • Approved pre-change baseline configuration of the applicable production Cyber Asset. • Implemented cyber security controls, and the state of each control pre-change. • Tool or Cyber Asset exports that reflect status of tested security controls and the pass/fail results of overall testing • Post-change baseline configuration of the production Cyber Asset • Automated comparisons of the pre-change and post-change baselines of the production Cyber Assets identifying variances. • Post-change cyber security controls, and the state of each control pre-change. • Comparison of pre- and post-change cyber security controls, and testing results demonstrating implementation aligns with expected state. Documentation of any associated actions to address identified issues. • If a test Cyber Asset is used, dated <i>system-generated</i> evidence of: <ul style="list-style-type: none"> ○ Pre-change baseline configuration of the test Cyber Asset ○ Records documenting known differences between production and test Cyber Assets ○ Records documenting considerations taken to account for or known differences ○ Post-change baseline configuration of the test Cyber Asset ○ Records documenting the differences between the pre-change and post-change baseline of the test Cyber Asset



Recommended Application Guidance – Potential Approaches (continued)	
Operational Controls Samples:	<ol style="list-style-type: none"> 1. On a cycle pre-defined by the Registered Entity, the SME will review the generated security survey questions to ensure they are still applicable and matches the requirements. 2. On a cycle pre-defined by the Registered Entity, if the system automatically gathers baseline information, the SME will test and validate the information for accuracy.
Manual Options	
<p>A manual approach can allow for inconsistency which is why a survey or questionnaire should be created using a tool such as Microsoft Excel to identify and document if the change can affect any security controls. Below is an example questionnaire that be used to identify possible affected controls.</p> <p>Following a change, the SMEs should verify that the security controls were not adversely affected by testing and documenting the results in whatever manual format (i.e. checklist, survey, form, or questionnaire) is used.</p> <p>If the manual format does not include a section that captures the variances between testing and production environments, the SME should create and maintain a document identifying any differences between the test and production environment including steps to mitigate the differences to attach to the record.</p>	
Tip:	Using a central repository to track baseline information and track changes such as Excel or SharePoint can help standardize processes and data without adding a lot of complexity. This approach also helps manage access security and information protection prescribed by CIP-004-6 and CIP-011-2.
Lessons Learned:	If the differences between the test environment and the production environment are contained in a separate document, Registered Entity’s may want to consider implementing processes that cause it to be updated after tested changes are promoted to production and reviewed periodically to ensure it is up to date for use the next time baseline changes need to be performed
Evidence:	<p>An approved Change Request; inclusive of pre-cautionary measures taken if a test environment is not used, the CIP-005 & CIP-007 security controls that may be impacted by the change, and the state each control is expected have upon completion of the change.</p> <p>Registered Entities should also consider capturing and retaining dated manually generated records of:</p> <ul style="list-style-type: none"> • Approved pre-change baseline configuration of the applicable production Cyber Asset. • Security controls to test following the change, and the state each control is expected have upon completion of the change. • Pre-cautionary measures taken if a test environment is not used. • Records documenting the status of tested security controls and the pass/fail results of overall testing • Post-change baseline configuration of the production Cyber Asset • Records documenting the differences between the pre-change and post-change baselines of the production Cyber Assets



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
Evidence: (continued)	<ul style="list-style-type: none"> • If a test Cyber Asset is used, dated records of: <ul style="list-style-type: none"> ○ Pre-change baseline configuration of the test Cyber Asset ○ Records documenting known differences between production and test Cyber Assets ○ Records documenting considerations taken to account for or known differences ○ Post-change baseline configuration of the test Cyber Asset ○ Records documenting the differences between the pre-change and post-change baseline of the test Cyber Asset
Exhibits:	See Exhibit P: Part 1.5. – Testing High Impact Baseline Changes (Manual Options) for a sample pre-testing questionnaire.
Operational Controls Samples:	On a cycle pre-defined by the Registered Entity, the SME will review and validate the pre-testing questionnaire/checklist to ensure the tasks still matches the requirements.



CIP-010-2, REQUIREMENT R2 – CONFIGURATION MONITORING

Analysis, Requirement R2. Configuration Monitoring

Requirement Language	
<p>R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].</p>	
Evaluation	
Objective:	<p>The objective of Requirement R2 is to cause Registered Entities to monitor certain controls implemented to comply with Requirement R1 for High Impact Applicable Cyber Assets/Systems and associated Cyber Assets to assure Configuration Change Processes are effectively implemented and operating as designed and to detect instances that deviate from documented process(es).</p>
Value Proposition:	<p>Monitoring Establishing baselines allows Registered Entities to identify significant changes to trigger change control, configuration management, and security assessment and testing procedures. Other benefits of having established configuration baselines for applicable Cyber Assets, either the individual host level or for a given category of infrastructure, include knowledge and awareness about:</p> <ul style="list-style-type: none"> • Known and expected state • Needed operational settings/parameters • Security design and posture <p>Changes that affect attributes of established baselines for any Cyber Asset come with some level of risk. Whether the change is intended to adjust functionality or feature sets, address a security vulnerability, and/or fix an operational performance issue; implementing changes can introduce unexpected/unintended results that could negatively impact operational security controls.</p> <p>Knowing the expected configuration baseline of a Cyber Asset is an important first step toward assessing and mitigating this risk. Effectively monitoring, managing, and approving changes to established baselines are equally important.</p>
Recommended Application Guidance – Potential Approaches	
<p>To support achievement of compliance at the main requirement level, a process could be characterized as a collection of interrelated tasks intended to solve a particular problem or perform a particular function. Processes typically describe the organizational accountability and sequencing of tasks to accomplish specific actions focusing on the input and output of the action, as well as what data and information flows through the process.</p> <p>Documented Configuration Monitoring processes may be used to provide a standardized enterprise or cross-functional framework on what phases are expected to be executed in what order when the process is operating as designed. This may help identify interdepartmental dependencies and/or where systems and human actions intersect. Several industry best practices and frameworks (as referenced in the Methodology section of this SAG) can serve as a guideline to establishing a robust process that also accomplishes the objective and minimum mandatory obligations within CIP-010-2 Requirement R2.</p>	



Recommended Application Guidance – Potential Approaches (continued)

Process documents may also be supported by instructional steps detailed at a Standard Operating Procedure (SOP) level, or a Departmental Operating Procedure (DOP) level, depending on the Registered Entity’s organizational structure, applicable Cyber Assets/Systems, and operational or technical nuances between departments. Processes may include narratives as well as illustrations or can also be in the form of standalone narrative documents, or independent documents that depict a work flow or process diagram.

Whichever process(es) or tools your organization implements, ease of use and consistency is key to success. Consideration of the following items may serve to help reduce risk and shape or guide the chosen approach toward a solution that is repeatable, sustainable, and works best for your organization:

- Where populations of applicable Cyber Assets are significant, without an automated monitoring system processing administrative reviews of voluminous data may result in human errors that could cause unauthorized changes to go unidentified. Undetected unauthorized changes to baseline configuration could unintentionally disrupt reliability if all the potential effects or dependencies of the change are not evaluated, or if the change was intended to do harm.
- Consider how the configuration monitoring intersects with incident response processes and emergency changes.
- Consider whether the configuration monitoring process is best managed; centrally or as a distributed process. For instance, control center EMS/SCADA systems may utilize one method to detect unauthorized baseline configuration change and systems designed to control and monitor electronic access to and through the ESP may use another.

If technology is used, it is recommended that the configuration monitoring system(s) have the capability to distribute automated reminders to SMEs and track required monitoring intervals and help remove human factors that could impact successful detection of unauthorized changes and/or timely response to unforeseen outcomes.

<p>Tip 1:</p>	<p>Consider adding check points in the configuration monitoring process to identify if change management processes are affected by the detection of an unauthorized change.</p> <ul style="list-style-type: none"> • For instance, detection of a baseline configuration change that was authorized outside of the primary system when the change management system was undergoing maintenance may appear to be an unauthorized change when it is not. Evaluating detected variances against processes may highlight the need to document alternative acceptable methods for authorizing change when primary mechanisms are not available.
<p>Tip 2:</p>	<p>Consider intersecting configuration monitoring process with incident response plans, and/or or disaster recovery plans to assure reporting obligations are met and compliance is maintained.</p> <ul style="list-style-type: none"> • For instance, investigations of detected unauthorized changes could warrant the activation of those plans, could lead to the declaration of a Reportable Cyber Security Incident, and/or could trigger associated 60/90-calendar day timeframes for updates to said plans; therefore, consider noting CIP-008 interaction in CIP-010 documentation.



Recommended Application Guidance – Potential Approaches (continued)	
Lessons Learned:	<p>Successfully implemented controls to detect unauthorized changes to baseline configurations do not obviate a Registered Entity’s obligation to comply with CIP-010-2 Requirement R1 Part 1.3 to authorize deviations from approved baselines. The longer the cycle between the execution of monitoring processes, the longer the time to detection of potential unauthorized changes, the greater the potential security risk and opportunity to do harm if actual unauthorized baseline changes are present and undetected, and the greater the duration of non-compliance with CIP-010-2 Requirement R1 Part 1.3 where unauthorized baseline configuration changes occurred. To minimize exposure and adverse impacts to reliability, Registered Entities may want to consider leveraging 3rd Party Tools to detect and alert on a cycle more frequent than the minimum obligation to reduce operational risk, security risk, and compliance risk.</p>
Evidence:	<p><u>Process Records:</u></p> <ol style="list-style-type: none"> 1. Documented Process(es): Registered Entities should establish and retain copies of the implemented process(es) narrative(s) and/or diagram(s) that collectively include Requirement R2 and Part 2.1. Where process(es) are documented in both narrative form and process flow diagrams, Registered Entities are best served to assure the two align. Some considerations to help assure sufficiency of this evidence includes producing dated process(es) and approval records that capture attributes such as Revision History, Effective Date, Approver Name/Role, Approval Signature, and Approval Date. Registered Entities may define the approver as an individual or a committee. <ul style="list-style-type: none"> • Revision History: Demonstrates the life and maturity of the process(es). Helps to demonstrate compliance timeframes for review cycles or necessary updates are met and that a Registered Entity is continuously improving process(es) and maintaining alignment between documented expectations and operational practices. • Effective Date: Demonstrates the expectation for when the process(es) are to be fully implemented and operationalized and provides reasonable assurance that the process(es) were established and available for use on or before the date the Standard Requirement(s) became effective and enforceable. • Approver Name/Role: Helps assure the person(s) approving the process operates in a position with the authority and resources to prioritize work and operationally execute in conformance with the documented configuration change management activities. • Approval Signature: A wet ink signature(s) or a digital approval(s) provides reasonable authentication of the signer and demonstrates that leadership in alignment with the intent, purpose, and activity prescribed by the CIP Requirement(s) and process(es). For sufficiency, the signature should be that of the Approver Name/Role or another employee that serves as that person’s/department’s leader (i.e. the Manager’s Director, or VP etc.) • Approval Date: Demonstrates process(es) were established and approved on or before the date the Standard Requirement(s) became effective and enforceable. For sufficiency, Approval Date should be on or before the Effective Date to demonstrate leadership awareness and agreement with implementation timing.



Recommended Application Guidance – Potential Approaches (continued)

<p>Evidence: (continued)</p>	<p>2. Potential Supporting Process Attributes/Content: Cyber Asset scope, Functional Area Accountability, and Roles and Responsibilities documentation, either within the process(es) or in a referenced document or tool (such as an Accountability Matrix) can help demonstrate the process(es) are communicated and implemented thereby reducing the risk of human performance errors. If this practice is used, this documentation should be dated and retained as compliance evidence with the process(es) records.</p> <p><u>Potential Supporting Records</u></p> <ol style="list-style-type: none"> 1. A Requirement Mapping, either within the process itself or as a separate supporting record, can help provide traceability between the steps or elements of the process(es) and each applicable Requirement Part to help assure collective inclusion of all necessary components in demonstration of compliance with each part. 2. Process and/or Workflow Diagrams for technologies/tools that govern, automate, or otherwise have a role in the execution of the documented process(es). This type of artifact can illustrate the sophistication of technical internal controls and help to demonstrate repeatability of the process used to comply. 3. Artifacts in combination from systems or manually executed activities can be used in concert to demonstrate implementation of the documented process(es); inclusive of collective evidence like, but not limited to, a: <ul style="list-style-type: none"> • Dated population of applicable Cyber Assets either manually created or from an inventory/asset management system, • Dated monitoring outputs for applicable Cyber Assets detailing status of the baseline at the time of each check, and demonstrating the check is performed on the required cadence of at least once per 35 calendar-days for the affected population, • Baseline change requests and approvals dated to occur during the monitoring period demonstrating the population of known authorized changes, accompanied by • Manual or system-generated comparison results of the monitoring outputs to the change records identifying detected unauthorized changes collectively show the auditor that process(es) are operationalized.
---	--



Recommended Application Guidance – Potential Approaches (continued)	
Operational Controls Samples:	<ol style="list-style-type: none"> 1. Prior to the enforcement date of CIP-010-2 R2 for applicable Cyber Assets/Systems, the owner(s) of applicable Cyber Assets/Systems establish approved processes that collectively include monitoring cycles and mechanisms for established baselines on a minimum periodicity of at least once per 35 calendar days, practices to identify and document potential unauthorized baseline configuration changes, and investigative response processes actions for actual detected unauthorized baseline configuration changes. 2. Per occurrence, approved process(es) are communicated to SMEs with a role in configuration monitoring and published in a repository that provides SMEs access to the process(es). 3. At a minimum, on a cycle of once per 15 calendar months, or more frequently based on need, the process owner(s), in collaboration with the affected SMEs, performs a review of the documented process(es), updates as needed to align with compliance requirements and operational practices, and executes procedures for re-approval and publication of revised processes to assure organizational alignment and availability of expected practices for SMEs. 4. At a minimum, on a cycle of once per 15 calendar months, or more frequently based on need, and where 3rd Party Tools are used to support the execution of configuration monitoring processes, the process owner(s), in collaboration with the affected SMEs, performs a gap analysis between the documented process(es) and the supporting technology to assure alignment between documented expectations and implemented technical controls within supporting 3rd Party Tools. 5. At a minimum, on a cycle of once per 15 calendar months, or more frequently based on need, the process owner(s) document any identified variances between established processes, operational practices, and/or supporting technology, provides management with recommendations to address variances; establishes, executes, and tracks status of a dated plan to align the documented processes to implemented practices and technology; and informs the compliance team of any potential instances of non-compliance for evaluation and reporting (if needed) to assure controls are effectively designed, operating as intended, and regulatory obligations are met.
3rd Party Tool Options	
<p>A configuration monitoring system typically supports the execution of a documented process and may be in the form of 3rd Party Tools like but not limited to an existing inventory management system with configuration monitoring and alerting capability, a configuration change authorization and tracking system, or even a custom application(s). Due to potential technical limitations, Registered Entities do not have to implement a 3rd Party Tool to accomplish compliance; however, it should be noted the SDT explicitly stated intent in Guidelines and Technical Basis¹⁵.</p>	

¹⁵ **Requirement R2:** The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring is not possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options Continued	
Tip:	The minimum obligation is to monitor on a minimum cycle of once per 35-calendar days; however, Registered Entities implementing technology to automate this process may want to consider configuring the tool for continuous monitoring in combination with leveraging automated alerting capabilities to increase timely visibility into potential issues, reduce security risk, decrease the duration of time a detected unauthorized change is implemented, and reduce the risk of non-compliance associated to unauthorized baseline changes.
Lessons Learned 1:	<p>Configuration monitoring process often rely on integrated systems and data sources. Consider implementing mechanisms to identify if monitoring capabilities are affected by changes or adjustments to integrated systems (i.e. change control systems, inventory management systems, security event information monitoring systems) that the configuration monitoring tools use (or rely upon) to detect unauthorized changes.</p> <ul style="list-style-type: none"> For instance, an inventory management system containing a binary value to identify Cyber Assets as a High Impact BES Cyber Asset undergoes a software enhancement that changes the position of that attribute within the database tables, and the configuration monitoring tool is no longer monitoring the intended population.
Lessons Learned 2:	Providing system-generated evidence from the 3rd Party Tool or the population of Cyber Assets requiring monitoring to support attestations that no unauthorized changes were detected for the monitored timeframe can increase credibility of the records and help reduce potential audit scrutiny.
Evidence:	<p><u>Configuration Monitoring Records</u></p> <ul style="list-style-type: none"> Artifacts from inter-related and/or integrated 3rd Party Tools when used in concert demonstrate the operational effectiveness of configuration monitoring; inclusive of collective evidence like, but not limited to, a: <ul style="list-style-type: none"> System timestamped exports of the population of applicable Cyber Assets from an inventory/asset management system (or the monitoring tool if it is the same system), System timestamped monitoring outputs from the 3rd party tool detailing baseline attributes at the time of each check, and demonstrating the check is performed on the required cadence of at least once per 35 calendar-days for the affected population, Baseline change requests and approvals dated to occur during the monitoring period demonstrating the population of known authorized changes, <i>System-generated</i> comparison results of the monitoring outputs to the change records identifying detected unauthorized changes collectively show the auditor that process(es) are operationalized, System timestamped journal entries, alert acknowledgements, comments, or other logged data demonstrating investigative response actions to detected unauthorized baseline configuration changes.



Recommended Application Guidance – Potential Approaches (continued)

3rd Party Tool Options (continued)

<p>Evidence: (continued)</p>	<p><u>Supporting Configuration Monitoring System Settings</u></p> <ul style="list-style-type: none"> • Artifacts that depict the settings configured within the 3rd Party Tool(s) further demonstrate processes are implemented and operating in alignment with regulatory obligations. For instance, exports or screenshots of the 3rd Party Tool’s: <ul style="list-style-type: none"> ○ Configured time source, whether local, ntp server, or gps clock lends credibility to any other <i>system-generated</i> evidence produced to demonstrate compliance, ○ Configured monitoring interval demonstrates the process occurs at least once every 35 calendar days. ○ Hosts configured in the querying settings provides traceability between the Cyber Assets the tool is monitoring and the population of Cyber Assets and Applicable Systems that require monitoring, ○ Attributes that the query checks for demonstrates that automated processes collectively include attributes defined by Requirement R1 Part 1.1.1 – 1.1.5, ○ Configuration to cause query return data to be compared to the approved baselines (where the 3rd party has the capability to store approved baselines) can demonstrate that automated processes can detect and distinguish between potential unauthorized changes and actual unauthorized changes. ○ Logs from the 3rd Party Tool, or other sources from data transport or access control devices between the 3rd Party Tool and the monitored Cyber Assets (i.e. EAPs or EACMSs) that capture the scheduled monitoring queries. ○ Evidence of the system configuration integration, scripts, or ingestion logic (where 3rd Party Tools may not have the capability to store approved baselines, but support integration with other baseline or change ticket data sources or the automated consumption of data feeds from other data sources) can demonstrate that automated processes can detect and distinguish between potential unauthorized changes and actual unauthorized changes, and/or.
<p>Operational Controls Samples:</p>	<ol style="list-style-type: none"> 1. On a cycle of a minimum of once per 35 calendar days, or more frequently based on need, the 3rd Party Tool queries the High Impact BCAs, and associated PCAs, and EACMSs, for changes to baseline attributes and autogenerates a report that is sent via email to system administrators for investigation. The email includes instruction for response, documentation of investigative results, and associated actions to address events that constitute unauthorized baseline configuration changes. 2. On a cycle of a minimum of once per 35 calendar days, management evaluates the outcome of investigations related to detected changes to baseline attributes and reports any events that constitute unauthorized baseline configuration changes to the compliance department for processing and external reporting of conditions of potential non-compliance. <p>Rationale: The next four ideas for internal controls contain cycles and timeframes that are <u>not</u> prescribed within the Requirements and are intended to illustrate some examples of potential ways a Registered Entity, through a focus on security best practice, could add rigor and compliance margin to their program using detective controls.</p>

Recommended Application Guidance – Potential Approaches (continued)



3rd Party Tool Options (continued)	
Operational Controls Samples: (continued)	<p>Some of these ideas consider cycles with a frequency more often than the baseline update interval that must occur within 30 calendar days as prescribed by CIP-010-2 Requirement R1 Part 1.3 and the monitoring interval to detect unauthorized changes that must occur every 35 calendar days as prescribed by CIP-010-2 Requirement R2 Part 2.1. Registered Entities who are interested in adding layers of safeguards may leverage these options, in any combination, to minimize the duration that unauthorized deviations from baselines are implemented and gain greater visibility into security posture and risk than the minimum requirements may achieve.</p> <ol style="list-style-type: none"> 1. On a cycle of once per week, as a secondary measure to minimize the potential for unauthorized changes, the Change Advisory Board, meets with SMEs and conducts a review of change requests in flight to assure a) authorization records exist and b) any new device implementations include tasks to account for them within the systems integrated into the 3rd Party Tool responsible for monitoring. 2. On a cycle of once per calendar day, as a secondary measure to assure monitoring tools can operate as required, the 3rd Party Tool automatically consumes a data feed from the Cyber Asset inventory system and executes a keepalive query to ascertain communication status with the population of Cyber Assets requiring configuration monitoring. For the tool autogenerates a report containing any unreachable systems and autogenerates a ticket to the system administrator on call to investigate why the system can no longer monitor. Tickets generate an automated email notification daily until the condition is resolved. 3. Upon exceedance of a 7-calendar day threshold for continuous loss of monitoring, as a tertiary management practice to assure system administrators respond and resolve conditions for any unreachable systems, the tool autogenerates an escalation ticket and high priority email notification to leader of the responsible functional area. Tickets generate an automated email notification daily until the condition is resolved. 4. On a cycle of once per calendar year, to provide reasonable assurance that unauthorized changes are detected, the internal audit department reviews approved processes, requests a full population of Cyber Assets and Applicable Systems requiring monitoring, takes a 10% sample of the population, requests a full population of approved baseline configuration change records for the sample, and compares it to an export of monitoring queries and detected events from the 3rd party monitoring tool.
<u>Manual Options</u>	
Registered Entities that choose to accomplish compliance with configuration monitoring requirements should be advised that the SDT explicitly stated intent for automated monitoring in the Guidelines and Technical Basis ¹⁶ for Requirement R2 and may want to consider establishing a road map to re-evaluate 3rd Party Tools to augment or replace manual processes over time.	

¹⁶ **Requirement R2:** The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.



Recommended Application Guidance – Potential Approaches (continued)	
Manual Options (continued)	
Where technical limitations preclude the use of automated solutions, other options that could be considered less sophisticated in nature might leverage administrative tools, like but not limited to, a standalone database or spreadsheet of Cyber Asset populations and/or authorized baselines, manually populated change control forms, monitoring schedules and checklists, review and comparison processes, governance, and records using paper forms or office productivity applications and meetings or email communications to track issues and actions.	
Tip 1:	If choosing to use a manual process to monitor for baseline configuration changes, create a list of configurations to monitor ahead of time and procedures on how to conduct monitoring.
Tip 2:	If choosing to use a manual process to monitor for baseline configuration changes, create a list of accountable SMEs, a standardized practice for communication of detected instances, and clear response expectation and timeframes for detected unauthorized baseline configuration changes to assure consistency, priority, and timeliness of response.
Lessons Learned:	Providing system-generated evidence (i.e. screenshots, exports, or commands otherwise captured to a file) from Cyber Assets accessed to perform manual monitoring activities to support attestations that no unauthorized changes were detected for the monitored timeframe can increase credibility of the records and help reduce potential audit scrutiny.
Evidence:	<p><u>Configuration Monitoring Records</u></p> <ol style="list-style-type: none"> 1. Artifacts used to manually perform configuration monitoring activities demonstrate the operational effectiveness of the process. Examples of collective evidence are like, but not limited to: <ol style="list-style-type: none"> a. A dated copy of the inventory list of High Impact BCAs, and associated PCAs, and EACMSs b. Dated copies of all approved change control records from the past 35 calendar days c. Dated copies of approved baseline configurations, d. Dated <i>system-generated</i> evidence from each Cyber Asset of the actual configured baseline attributes e. Documented identified variances, inclusive of the date of detection f. Dated records of communication to responsible system administrator(s) for investigation of potential unauthorized baseline configuration changes. g. Dated records of response actions, documentation of investigative results, and associated mitigating or corrective actions to address events that constitute unauthorized baseline configuration changes.
Operational Controls Samples:	<ol style="list-style-type: none"> 1. On a cycle of a minimum of once per 35 calendar days, the system baseline monitoring SME detects unauthorized changes to baseline configuration by retrieving the inventory list of High Impact BCAs, and associated PCAs, and EACMSs, and for each Cyber Asset on the inventory list: <ol style="list-style-type: none"> a. Pulls all approved change control records from the past 35 calendar days, b. Collects records of approved baseline configurations, c. Uses authorized access to connect to each Cyber Asset, and manually verifies that <ol style="list-style-type: none"> i. The configured baseline matches the documented and approved baseline, or ii. Deviations between the configured baseline and the documented and approved baseline are authorized within an approved change request.



Recommended Application Guidance – Potential Approaches (continued)

Manual Options (continued)

<p>Operational Controls Samples: (continued)</p>	<p>Where baseline changes cannot be verified as authorized, the system baseline monitoring SME documents the detected variances and sends an email to the responsible system administrator(s) for investigation. The email includes instruction for response, documentation of investigative results, and associated actions to address events that constitute unauthorized baseline configuration changes.</p> <p>Similar to the Rationale for Requirement R2 and 3rd Party Tools within the Operational Controls Samples Section of this analysis, the next four ideas for internal controls contain cycles and timeframes that are <u>not</u> prescribed within the Requirements and are intended to illustrate some examples of potential ways a Registered Entity, through a focus on security best practice, can minimize the risk associated to human performance errors and gain compliance margin within their program using detective controls.</p> <ol style="list-style-type: none"> 1. On an ongoing basis, the system baseline monitoring SME maintains a register of detected unauthorized changes to baseline configuration and contacts the responsible system administrator once per week to obtain status. 2. On a cycle of once per month, using the register of detected unauthorized changes to baseline configuration, the system baseline monitoring SME generates a report and associated metrics that is provided to leadership and the compliance team detailing any detected unauthorized changes, the status of those changes, and the risk, timing and action plans to resolve each. 3. On a cycle of once per month, leadership reviews the report of detected unauthorized changes and associated metrics assesses the risk and prioritizes and redirect resources as needed to resolve each. 4. On a cycle of once per month, the compliance team reviews the report of detected unauthorized changes and associated metrics, assesses the risk, executes processes for reporting potential instances of non-compliance to the regulator, evaluates mitigation plans for sufficiency, recommends potential process improvements or corrective actions to leadership for consideration.
---	---



CIP-010-2, REQUIREMENT R2 – CONFIGURATION MONITORING

Analysis, Part 2.1 – Monitoring Baselines for Unauthorized Changes

CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
Evaluation			
Objective:	The objective of routine monitoring of baseline configuration pursuant to Requirement R2 Part 2.1 is to assure unauthorized baseline changes are detected, investigated, and remediated. This built in detective control helps assure the security posture is known and maintained, and that baseline deviations are implemented in accordance with change control processes.		
Value Proposition:	Routine monitoring of baseline configurations serves as a detective control for unexpected and/or unauthorized changes, as well as potential Cyber Security Incidents. Detection triggers investigative actions and provides the opportunity to restore baselines to a secure known state. Prompt detection, response, and recovery serves to mitigate potential risk of security vulnerabilities that can be introduced by unapproved changes that deviate from the baseline.		
Recommended Application Guidance – Potential Approaches			
<p>Requirement R2 is only applicable to High Impact BES Cyber Systems and associated EACMS and PCA. Most High Impact BES Cyber Systems have a significant number of Cyber Assets and therefore it can be a daunting challenge to monitor for changes to the baseline configuration at least once every 35 calendar days.</p> <p>There are many technical ways to accomplish Requirement R2 Part 2.1; however, that does not preclude a Registered Entity from employing a manual approach. The best solution is one that aligns with an organizations resource base and works in each individual environment. This section includes many things to consider when determining a course of action to meet Part 2.1. No matter which process you employ be sure to have a program narrative(s) that documents your process as this is essential to demonstrate compliance. Whether using technology, a manual approach, or a hybrid solution, assure it is repeatable and sustainable.</p> <p>In some cases, a 3rd Party Tool may be used to gather baseline information, but the tool may not be capable of maintaining the baseline information. In this case the baselines are maintained in a separate repository. Even if the tool is capable of documenting the baselines an entity may choose to only use the tool to gather the information and have the comparison function processed elsewhere, either automatically or manually. If this is the case, your baseline monitoring function may be occurring by a completely separate program or possibly the program utilized as the baseline repository. This type of approach may be chosen when an in-house program is to be utilized to allow greater flexibility over the features provided in a 3rd Party Tool alone.</p>			



Recommended Application Guidance – Potential Approaches (continued)	
<p>There is nothing wrong with this approach as long as the system is meeting the compliance obligations and is able to produce auditable evidence.</p> <p>Whether using 3rd Party Tools, a Manual approach, or a Hybrid solution, assure your process(es) include documenting and investigate detected unauthorized changes. Changes are going to happen within a control system environment that will affect Cyber Asset baselines, such as security patches or application upgrades or new application installations. These events are necessary and a normal occurrence in the life of the system. Depending on how often your monitoring system performs baseline configuration change detection, you may receive an alert that a Cyber Asset has changed.</p> <ul style="list-style-type: none"> • If the change is authorized and documented within 30 calendar days of the change (CIP-010-2 Requirement R1 Part 1.3) there should be no reason for concern as long as those approvals are documented, and baseline updates are completed. • If the baseline change has not been authorized investigate and document the change. Depending on the findings of the investigation consider if the Cyber Security Incident Response Plan (CIP-008-5) needs to be activated to determine if there has been a Cyber Security Incident. 	
Tip 1:	<p>Effective implementation of R2.1 can also serve as a Key Risk Indicator (KRI) for the implementation status and maturity of Change Control Processes. Similarly, this data could be trended over time and serve as a Key Performance Indicator (KPI). These are side benefits a Registered Entity may want to consider if developing metrics and/or providing dashboards to illustrate performance to leadership or accountable functional areas that perform day-to-day operational activities to achieve and maintain compliance.</p>
Tip 2:	<p>Consider running the baseline validations more frequently than every 35 calendar days. Per CIP-010-2 Part 1.3, changes to a Cyber Asset that deviate from the existing baseline configuration need to be documented within 30 calendar days. Performing the Part 2.1 baseline validations more frequently and alerting on changes can be a good preventive control for Part 1.3.</p>
Tip 3:	<p>Even though complying with CIP-010-2 Requirement R2 is a built-in control for high impact only, the concept could be used as a control for medium impact Control Centers and/or substations to support compliance with CIP-010-2 Requirement R1 Part 1.1 – 1.4, which is applicable to medium impact. If a Registered Entity has, or will be, investing in 3rd Party Tools the high impact solution could be placed on a road map and leveraged over time as a holistic security strategy for medium impact. Registered Entities may want to consider a potential side benefit of early detection and prevention of potential non-compliance for medium impact for CIP-010-2 Requirement R1 Part 1.1 – 1.4. and overall consistency and continuous improvement as an enterprise solution.</p>
Lessons Learned:	<p>Requirement R2 acts as a reliability and compliance control for Parts 1.2 and 1.3 of the CIP-010-2 Standard.</p> <ul style="list-style-type: none"> • If a baseline change was not authorized, it does not relieve a Registered Entity from the compliance obligations under Part 1.2. • If a baseline change was authorized but the documentation has not been updated within 30 calendar days of the change, it does not relieve a Registered Entity from the compliance obligations under Part 1.3



Recommended Application Guidance – Potential Approaches (continued)	
Evidence:	<p>Whether using a tool or performing manual monitoring processes, Registered Entities should capture evidence that supports the outcomes and conclusions from the periodic execution of the monitoring process. Examples of artifacts needed to provide traceability to monitoring records:</p> <ul style="list-style-type: none"> • Dated population(s) of applicable Cyber Assets that require baseline configuration monitoring • Dates and approved baselines for the Cyber Asset population • Dated and approved baseline change request records relevant to the Cyber Asset population <p>Additional monitoring evidence is detailed in the respective 3rd Party Tool or Manual option sections for Part 2.1 later in this analysis.</p>
Operational Controls Samples:	<p>On a minimum cycle of once per 35 calendar days, and within 24 hours of the scheduled timeframe to monitor, the responsible SMEs collect and assemble records needed to support the execution of monitoring processes that detect unauthorized changes. These records include the applicable population of Cyber Assets, the current approved baselines, and any authorized change records.</p>
3rd Party Tool Options	
<p>Many entities have chosen to implement an automated solution to help manage their Cyber Assets since Requirement R2 was introduced in Version 5. An automated solution has the benefit of providing repeatable processes with little or no human intervention. This helps reduce human performance errors. The level to which automation can be utilized greatly depends upon the capabilities of the tool and the types and capabilities of the Cyber Assets. These 3rd Party Tools are some of the same tools you will find being utilized for normal business IT management functions like system inventory, vulnerability management, file integrity monitoring and security configuration management. The 3rd Party Tool selected should be able to perform compliance tasks for Part 1.1 and Part 2.1.</p> <p>Monitoring tools may come with built-in rules for specific CIP requirements. Keep in mind that the rules may need to be tuned to your environment. Some monitoring tools allow Cyber Asset baselines to be documented within the program itself. Detected changes to the baselines can then be directly alerted upon.</p> <p>Depending on your company’s in-house expertise, you may elect to build a completely custom automated monitoring program. There is nothing wrong with this approach as long as the system is meeting the compliance obligations and is able to produce auditable evidence.</p>	
Tip 1:	<p>The 3rd Party Tool could automatically gather baseline information and notify SMEs of any changes. The SMEs would then validate if the changes were planned or not.</p>
Tip 2:	<p>If baseline change alerts are sent via email, it is recommended that the alerts be sent to more than one address to make sure the alert is received in the event the primary support person is absent. Some monitoring tools may only show alerts on the management console.</p>
Tip 3:	<p>Where possible, when implementing a Security Information Event Management (SIEM) system, consider centralization and consolidation of distributed solutions to provide:</p> <ul style="list-style-type: none"> • Aggregated and correlated events and alerts, • A more holistic view of security posture and risk, • Standardization of end node configuration,



Recommended Application Guidance – Potential Approaches (continued)	
3rd Party Tool Options (continued)	
Tip 3: Continued	<ul style="list-style-type: none"> • Repeatable processes that generate consistent evidence to support audit, • Efficiency gains by removing the need to synchronize data and tuning configurations across multiple systems, and • To support cost prudence objectives.
Tip 4:	<p>Consider the sensitivity of the data and the capability of the monitoring system(s) when determining the logical placement and how it may affect the performance of the EAP, firewall rule configuration needs, as well as the Cyber Asset classification.</p> <ul style="list-style-type: none"> • If the tool is located within the ESP, firewall rules for monitoring through an EAP are not needed. A communication pathway to move data out of the ESP for compliance evidence may be required. • Conversely, if the monitoring system is located outside the ESP consider the security risk of needing firewall rules that allow the monitoring system to reach into the protected network to provide adequate monitoring capability to satisfy the requirement.
Lessons Learned 1:	When configuring or customizing 3rd Party Tools, and/or developing in-house applications, consider documenting the implementation for repeatability, cross training, and bench strength. This can assure expertise for ongoing support, maintenance, and tuning of the system. If augmenting staff with external resources for tool implementation, consider incorporating documentation and knowledge transfer into the project's Statement of Work.
Lessons Learned 2:	If a 3rd Party Tool is utilized, consider any CPU loading that may be placed on a system while interrogating it. While most systems these days typically have CPU horsepower to spare the consideration should not be overlooked. Also consider the effect of network scans on a system when verifying Part 1.1.4 (logical network accessible ports).
Lessons Learned 3:	As with any automated system things can still go awry. It is recommended to periodically test the system that is monitoring baseline changes. Most systems have built-in client monitoring capabilities commonly referred to as a "heartbeat" but unless you have configured regular emails from the management console or regularly check the console you may not be aware of a monitoring system failure.
Lessons Learned 4:	When implementing a 3rd Party Tool, consider how data can be extracted. Avoid assumptions that the software is configurable to allow and attributes in any combination to be combined and reported on. It is important to insist the vendor differentiate between out of the box configuration capability or reports, dashboards, or views vs customizations of data base queries or necessity to integrate with reporting tools to timely and repeatedly extract data. Asking about things like routine scheduled reporting as well as on demand querying based on specified date range parameters can help assure expectations are met and surprises are minimized when having to produce records for time sensitive Requests for Information.
Lessons Learned 5:	Requirement R2 acts as a reliability and compliance control for Parts 1.2 and 1.3 of the CIP-010-2 standard. <ul style="list-style-type: none"> • If a baseline change was not authorized, it does not relieve a Registered Entity from the compliance obligations under Part 1.2.



Recommended Application Guidance – Potential Approaches (continued)

3rd Party Tool Options (continued)

If a baseline change was authorized but the documentation has not been updated within 30 calendar days of the change, it does not relieve a Registered Entity from the compliance obligations under Part 1.3.

Evidence: 3rd Party Tool Outputs

A comprehensive suite of records could include the collective set of evidence listed herein; however, Registered Entities should consider that this list may not be all inclusive or entirely applicable to every 3rd Party Tool or its implementation and is intended as a guide to make informed decisions about what records in whole or in part may be sufficient.

This evidence list can also provide guidance for the feature sets to look for if designing and implementing a 3rd Party Tool and to configure it such that in-system evidence can be captured automatically when processing detected events. Implementing solutions that capture sufficient evidence as a part of normal operational activities alleviates the administrative overhead of having to prepare documentation as a separate compliance task.

The more supporting evidence a Registered Entity retains, the greater demonstration can be made that monitoring has been accomplished within the 35-calendar day timeframe. To demonstrate monitoring is effectively implemented and operating as designed on the minimum prescribed cycle, Registered Entities should consider retaining evidence of any:

Evidence Description	Rationale/Benefit
Detected potential unauthorized baseline deviations (i.e. application logs) inclusive of date and time stamp of detection, the subject Cyber Asset(s), and the affected baseline attribute(s).	<ul style="list-style-type: none"> • Demonstrates monitoring tools are operating as designed. • Demonstrates detected events include minimum information necessary to assess and address potential unauthorized changes.
Alerts, (i.e. <i>system-generated</i> evidence of alert logs, auto-generated incident tickets, and/ or emails inclusive of the date and timestamp the alert was sent and the content of the message)	<ul style="list-style-type: none"> • Demonstrates detected potential unauthorized baseline deviations are communicated timely to personnel responsible for assessing and addressing. • Demonstrates timeframes between system detection and responder awareness.

3rd Party Tool In-System Records

Evidence Description	Rationale/Benefit
Review or acknowledgement records that alerts were received, assessed, and addressed; inclusive of date and timestamp of the review or acknowledgement actions taken and any records that may have been generated to support the activation of Incident Response (if needed).	<ul style="list-style-type: none"> • Supports demonstration of compliance with CIP-008-5 if detected events met conditions to activate Incident Response Plans. • Demonstrates monitoring and alerting mechanisms are working as designed. • Demonstrates responders initiated investigative activities timely for any unauthorized changes that were detected and acted as needed.



Recommended Application Guidance – Potential Approaches (continued)										
3rd Party Tool Options (continued)										
Evidence: Continued	<p>3rd Party Tool Configuration</p> <p>Registered Entities may also want to consider retaining evidence of how the 3rd Party Tool is configured. Having dates system configurations can be particularly helpful in demonstrating compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. Being able to demonstrate to an auditor that the system was configured to monitor the correct population of applicable Cyber Assets, the minimum attributes requiring configuration change management, and the capability to detect and those conditions is helpful when having to prove a ‘non-event’. To follow are examples of these kinds of supporting records.</p>									
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Evidence Description</th> <th style="width: 50%;">Rationale/Benefit</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;"> <p>Dated system configurations of which Cyber Assets and which corresponding configuration attributes are monitored, inclusive of the cycle on which the monitoring is set to occur.</p> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> Provides traceability to the high impact BES Cyber Asset/System inventory and population of associated Applicable Systems to demonstrate monitoring is implemented for all in scope Cyber Assets. Demonstrates monitoring tools are configured for the five required baseline attributes. Demonstrates monitoring tools are configured for the minimum prescribed monitoring cycle Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. </td> </tr> <tr> <td style="vertical-align: top;"> <p>Dated system configurations of alert log retention intervals or forwarding parameters to send to a centralized SIEM.</p> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> Can serve as a secondary data source to help demonstrate monitoring was effectively implemented in scenarios where the 3d Party Tool may have retention limitations for detected events of potential unauthorized baseline deviations. Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. </td> </tr> <tr> <td style="vertical-align: top;"> <p>Dated system configurations to present alerts to a console/display and/or disseminate alerts to responders via alternate methods (i.e. email, text, incident tickets etc.).</p> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> Demonstrates the system is configured to alert for detected potential unauthorized baseline deviations Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. </td> </tr> <tr> <td style="vertical-align: top;"> <p>Dated authorizations corresponding to detected baseline changes that after investigation did not qualify as unauthorized, and baseline documentation updates.</p> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> May demonstrate compliance with CIP-010-2 Requirement 1 Part 1.2 if the detected change was authorized. May demonstrate compliance with CIP-010-2 Requirement 1 Part 1.3 for baselines documentation updates within 30 calendar days </td> </tr> </tbody> </table>	Evidence Description	Rationale/Benefit	<p>Dated system configurations of which Cyber Assets and which corresponding configuration attributes are monitored, inclusive of the cycle on which the monitoring is set to occur.</p>	<ul style="list-style-type: none"> Provides traceability to the high impact BES Cyber Asset/System inventory and population of associated Applicable Systems to demonstrate monitoring is implemented for all in scope Cyber Assets. Demonstrates monitoring tools are configured for the five required baseline attributes. Demonstrates monitoring tools are configured for the minimum prescribed monitoring cycle Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 	<p>Dated system configurations of alert log retention intervals or forwarding parameters to send to a centralized SIEM.</p>	<ul style="list-style-type: none"> Can serve as a secondary data source to help demonstrate monitoring was effectively implemented in scenarios where the 3d Party Tool may have retention limitations for detected events of potential unauthorized baseline deviations. Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 	<p>Dated system configurations to present alerts to a console/display and/or disseminate alerts to responders via alternate methods (i.e. email, text, incident tickets etc.).</p>	<ul style="list-style-type: none"> Demonstrates the system is configured to alert for detected potential unauthorized baseline deviations Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 	<p>Dated authorizations corresponding to detected baseline changes that after investigation did not qualify as unauthorized, and baseline documentation updates.</p>
Evidence Description	Rationale/Benefit									
<p>Dated system configurations of which Cyber Assets and which corresponding configuration attributes are monitored, inclusive of the cycle on which the monitoring is set to occur.</p>	<ul style="list-style-type: none"> Provides traceability to the high impact BES Cyber Asset/System inventory and population of associated Applicable Systems to demonstrate monitoring is implemented for all in scope Cyber Assets. Demonstrates monitoring tools are configured for the five required baseline attributes. Demonstrates monitoring tools are configured for the minimum prescribed monitoring cycle Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 									
<p>Dated system configurations of alert log retention intervals or forwarding parameters to send to a centralized SIEM.</p>	<ul style="list-style-type: none"> Can serve as a secondary data source to help demonstrate monitoring was effectively implemented in scenarios where the 3d Party Tool may have retention limitations for detected events of potential unauthorized baseline deviations. Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 									
<p>Dated system configurations to present alerts to a console/display and/or disseminate alerts to responders via alternate methods (i.e. email, text, incident tickets etc.).</p>	<ul style="list-style-type: none"> Demonstrates the system is configured to alert for detected potential unauthorized baseline deviations Helps demonstrate compliance with monitoring requirements when no unauthorized changes are detected within the 35-calendar day period. 									
<p>Dated authorizations corresponding to detected baseline changes that after investigation did not qualify as unauthorized, and baseline documentation updates.</p>	<ul style="list-style-type: none"> May demonstrate compliance with CIP-010-2 Requirement 1 Part 1.2 if the detected change was authorized. May demonstrate compliance with CIP-010-2 Requirement 1 Part 1.3 for baselines documentation updates within 30 calendar days 									
Exhibits:	<p>See Exhibit Q: Part 2.1 – Monitoring Baselines for Unauthorized Changes (3rd Party Tool Options) for screen shots of how a 3rd Party Tool may indicate a baseline attribute detected change.</p>									



Recommended Application Guidance – Potential Approaches (continued)	
Operational Controls Samples:	On a cycle of a minimum of once per 35 calendar days, or more frequently based on need, the 3rd Party Tool performs a query of High Impact BCAs, and associated PCAs, and EACMSs, for changes to baseline attributes and autogenerates a report that is sent via email to system administrators for investigation. The email includes instruction for response, documentation of investigative results, and associated actions to address events that constitute unauthorized baseline configuration changes
Manual Options	
<p>This method may be less costly from a product purchase standpoint and more labor intensive with a greater chance for human performance errors. If an automated tool was not utilized for Requirement R1 Part 1.1 then this is your most likely solution. The output gathered to fulfill developing baselines can be utilized to perform the required comparisons for monitoring. One approach could be to run a script to gather the operating system version of a Cyber Asset and perform a comparison between files. The comparison of the output files to the established baselines needs to be performed for each applicable subpart of Requirement R1 Part 1.1 on each high impact BCA, EACMS and PCA.</p> <p>If you have a significant number of Cyber Assets, scalability is an important consideration to help alleviate the administrative burden and human performance risk posed by manually performing activities and documenting compliance with Requirement R2 Part 2.1. For this reason, deploying an automated or Hybrid solution could be more repeatable and achievable if there are many Cyber Assets to monitor. Note: The Guidelines and Technical Basis section for Part 2.1 states: “The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System.” That said, the CIP SME Team has chosen to provide guidance to help those Registered Entities who may not have technology or automation available.</p>	
Tip 1:	If you have chosen to implement a manual monitoring process it is recommended that a task reminder system be utilized as a control to remind personnel of the 35-calendar day requirement. This could be something as simple as an Outlook calendar reminder or potentially part of a ticketing / work order management system.
Tip 2:	There are numerous programs that can perform a comparison function (https://en.wikipedia.org/wiki/Comparison_of_file_comparison_tools). The Registered Entity may already own some tools such as Microsoft Word. Microsoft Word has a very simple text file comparison function. The key is to utilize program that work in the Registered Entity’s environment and produce evidence that the comparison was made.
Lessons Learned 1:	Providing <i>system-generated</i> evidence to support attestations can increase credibility of manually created comparison/assessment records, helping reduce potential audit scrutiny.
Lessons Learned 2:	<p>Requirement R2 acts as a reliability and compliance control for Requirement R1 Parts 1.2 and 1.3 of the CIP-010-2 standard.</p> <ul style="list-style-type: none"> • If a baseline change was not authorized, it does not relieve a Registered Entity from the compliance obligations under Requirement R1 Part 1.2. • If a baseline change was authorized but the documentation has not been updated within 30 calendar days of the change, it does not relieve a Registered Entity from the compliance obligations under Requirement R1 Part 1.3



Recommended Application Guidance – Potential Approaches (continued)

Manual Options (continued)	
Evidence:	<p>In some cases, the Requirement R1 Part 1.1.1 evidence gathered for firmware based Cyber Assets may be a screen capture. In this case the monitoring would be a comparison based on a person visually checking the firmware version and comparing it to the original screen capture or a listing of the firmware version. Simplistic evidence of performing this task could be documenting the performance of this task by initialing a checklist and dating it. However, this type of documentation is merely an attestation. Consider supporting this evidence with a dated screen capture of the firmware version appended to the record to demonstrate actual system configuration in addition to the attestation. This is known as “stacked evidence” and provides clearer evidence of compliance.</p>
Operational Controls Samples:	<p>On a cycle of a minimum of once per 35 calendar days, the system baseline monitoring SME detects unauthorized changes to baseline configuration by retrieving the inventory list of High Impact BCAs, and associated PCAs, and EACMSs, and for each Cyber Asset on the inventory list:</p> <ol style="list-style-type: none"> 1. Pulls all approved change control records from the past 35 calendar days, 2. Collects records of approved baseline configurations, 3. Uses authorized access to connect to each Cyber Asset, and manually verifies that either: <ol style="list-style-type: none"> a. The configured baseline matches the documented and approved baseline, or b. Deviations between the configured baseline and the documented and approved baseline are authorized within an approved change request. <p>Where baseline changes cannot be verified as authorized, the system baseline monitoring SME documents the detected variances and sends an email to the responsible system administrator(s) for investigation. The email includes instruction for response, documentation of investigative results, and associated actions to address events that constitute unauthorized baseline configuration changes.</p>



MITIGATING RISK AND INTERNAL CONTROLS

Governance, Self-Monitoring, and Reasonable Assurance Options

The Registered Entity determines the depth and breadth of its internal controls. Internal Controls should be proportional to risk, to reasonably assure maintained alignment between day-to-day operational practices and a Registered Entity's stated expectations. Internal controls reduce opportunity for human performance errors and help establish roles to execute baseline configuration change management and monitoring processes, and to maintain the programs, supporting systems, associated inventories, and compliance records.

Registered Entities are encouraged to design and implement self-monitoring through internal controls, continuous improvement, and Corrective & Preventative Action Programs. When implementing internal controls, Registered Entities should consider organizational structure, the talents and skill sets of its resources, evaluate program maturity, contemplate establishing a road map to guide the organization's continuous improvement, and measure maturity over time.

Structure:

Registered Entities with a distributed compliance model (dedicated compliance experts embedded in each function) may be able to leverage distributed experts to provide self-assessments of operational conformance to internal controls for the function. Registered Entities with a centralized compliance model may be able to leverage centralized experts to provide more holistic compliance sufficiency self-assessments independent of the functional area responsible for executing operational controls. When determining who best to conduct a self-assessment of internal controls, Registered Entity's may want to also consider the nuance between activities intended to discover and remediate non-conformance vs non-compliance. In general terms, the nuance is as follows:

- Non-conformance can be considered any condition where a Registered Entity operates in a manner that is at variance with the words in approved and documented practices.
- Non-compliance can be considered any condition where a Registered Entity operates in a manner that is at variance with the words in the current enforceable mandatory regulation's Requirement(s).

Conditions of non-compliance are typically also conditions of non-conformance; however, not every instance of non-conformance may constitute non-compliance. For Registered Entities that choose to design programs with internal controls that are executed on a cycle more rigorous than the minimum CIP Requirements, detection of non-conformance could catch and remediate a condition before it rises to the level of a violation. This approach can add compliance margin, foster sound security practices, and mitigate security and compliance risk by reducing the duration of the issue.

Refer to [Appendix E](#) for additional ideas and examples of how to mitigate risk and leverage internal controls to support compliance with mandatory regulations



APPENDIX A: REFERENCES

Enforceable Regulations:

1. NERC Reliability Standard CIP-010-2 (Configuration Change Management and reliability Standards). Retrieved from: <http://www.nerc.com/files/CIP-010-2.pdf>
2. NERC Glossary of Terms. Retrieved from [NERC Glossary of Terms](#)

Industry Models, Frameworks, and Methodologies:

1. [CIS](#) (Critical Security Controls) for Security Controls for Effective Cyber Defense
2. [COBIT](#) (Control Objectives for Information and Related Technologies)
3. [COSO](#) (Committee of Sponsoring Organizations) of the Treadway Commission
4. [C2M2](#) (Cybersecurity Capability Maturity Model)
5. [ITIL](#) (Information Technology Infrastructure Library)
6. [NIST](#) (National Institute of Standards and Technology)
7. [OODA](#) (Observe, Orient, Decide, Act) Loop
8. [IIA](#) (The Institute of Internal Auditors)



APPENDIX B: ACRONYMN GUIDE

CEA	Compliance Enforcement Authority
BCA	BES Cyber Asset
BES	Bulk Electric System
BIOS	Basic Input/Output System
C2M2	Cybersecurity Capability Maturity Model
CCM	Change & Configuration Monitoring
CEC	CIP Exceptional Circumstances
CIP	Critical Infrastructure Protection
CIS	Critical Security Controls for Security Controls for Effective Cyber Defense
CMEP	Compliance Monitoring and Enforcement Program
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
EACMS	Electronic Access Control and/or Monitoring System
EAP	Electronic Access Point
ERC	External Routable Connectivity
ERM	Enterprise Risk Management
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
FTP	File Transfer Protocol
FW	Firmware
GPS	Global Positioning Satellite
GRC	Governance, Risk, and Controls
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICMP	Internet Control Message Protocol
ID	Identification
IIA	The Institute of Internal Auditors
I/O	Input/Output
IRA	Interactive Remote Access
IS	Intermediate System
ITIL	Information Technology Infrastructure Library
MCR	Material Change Report



NTP	Network Time Protocol
KB	Knowledge Base
MRO	Midwest Reliability Organization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OOB	Out of the Box
OODA	Observe, Orient, Decide, Act Loop
OS	Operating System
PACS	Physical Access Control System
PCA	Protected Cyber Asset
PCAC	Per Cyber Asset Capability
PCSC	Per Cyber System Capability
PSP	Physical Security Perimeter
RAS	Remote Access Server
RCM	Risk Control Matrix
RFI	Request for Information
SAG	Standard Application Guide
SDT	Standards Drafting Team
SMET	Subject Matter Expert Team
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Socket Shell
SW	Software
TCP	Transmission Control Protocol
TFE	Technical Feasibility Exception
UDP	User Datagram Protocol



APPENDIX C: GLOBAL EVIDENCE CONSIDERATIONS

Documented Configuration Change Management and Configuration Monitoring Processes are one component of demonstrating compliance with Requirement R1 and R2. To sufficiently satisfy each required element, and help provide clarity when undergoing an audit that process(es) collectively includes all minimum requirements, consideration of how each process maps to the details of each applicable requirement part in:

- CIP-010-2 Table R1 – Configuration Change Management, and
- CIP-010-2 Table R2 – Configuration Monitoring

While official approvals of the process are not mandated by the requirement, consider implementing governance practices that capture approval records and versioning. This may improve the chance that those responsible for executing the process(es) have confidence that it is codified by their leadership and their roles and responsibilities are clear.

Having evidence of the date the process(es) was approved and became effective is necessary to demonstrate each was established within compliance timeframes. Revision history within the process document itself, or through electronic versioning mechanisms/workflows in a document management system are helpful to demonstrate compliance, though there are other mechanisms that can be employed to demonstrate approval and publication, like email approval records, dated 'wet-ink' or digital signatures, appended approval forms, etc.

Performing documentation reviews and updates on a predefined cycle or based on triggering events like project-related process or technology changes, can help produce dated evidence to further demonstrate to an auditor that the process documentation is up-to-date and understood.

Consider designing processes that generate evidence as a byproduct of executing the process. One potential approach to accomplish this is to include sections within related operating procedures to define expected evidence, coupled with instructions on what to capture at the time of execution for sufficient demonstration of compliance. Consider setting expectations that documented evidence is formatted as prescribed by the Registered Entity's definitions, using required manually documented records (like forms, checklists etc.), or satisfied through equivalent system outputs or reports already sufficiently designed and implemented to do so.

In addition to capturing completed versions of any manually documented records, consider capturing applicable supporting narrative documentation (plans, procedures etc.) and/or system-generated evidence proving the implementation and execution of activities that align with approved processes.

Demonstrating the implementation of the documented process(es) requires additional evidence for which examples are provided within each section of this SAG that focuses on the Requirement Part. The below high-level summary of the types of dated records that may help a Registered Entity sufficiently demonstrate compliance with the enforceable version the CIP-010-2 Reliability Standards is as follows:

- Dated review, and where applicable, approval records for plans, processes, procedures, and documented administrative or technical systems or methods implemented as part of the configuration change management Program.
- Dated change request and approval records, including *system-generated* evidence to demonstrate the implementation or roll back of approved baseline changes.
- Dated Cyber Security control testing records, including *system-generated* evidence to demonstrate the configuration and functionality of pertinent security controls.



APPENDIX C: Global Evidence Considerations Continued

- Dated configuration baselines and dated revision history, either by individual Cyber Asset or by Cyber Asset grouping; inclusive of affected Cyber Asset attributes to reflect alignment between configuration changes and documented baselines
- Dated document revision history to reflect alignment between configuration changes and incident response and recovery plan updates and communications, including dated communication records.
- Any additional lists or records required to support demonstration of the implementation of configuration change management processes, that may include, and may not be limited to, dated records like:
 - inventories or diagrams of applicable Cyber Assets/Systems, ESPs, or PSPs,
 - lists of baseline change approvers,
 - lists of cyber security controls assessed for baseline changes; test records may include supporting lists of:
 - centralized or otherwise interdependent systems or applications
 - connectivity characteristics (serial, ERC, IRA, Dial-up)
 - configured accounts, users, and associated controls etc.
 - lists of operating systems/firmware inclusive of installed versions,
 - lists of intentionally installed commercial, opensource, or custom software,
 - lists of approved and/or open network accessible logical ports,
 - lists of applicable and/or installed security patches,
 - lists of approved Technical Feasibility Exceptions (TFEs) and covered applicable Cyber Assets/Systems, and associated mitigation records (if any TFEs are active),
 - lists of Cyber Assets that have been identified having technical limitations or preclusions that require the use of TFE provisions,
 - lists of Cyber Assets that have been identified as not being capable of a particular function where the provision for Per Cyber Asset Capability (PCAC) exists, and/or
 - lists of Cyber Systems that have been identified as not being capable of a particular function where the provision for Per Cyber System Capability (PCSC) exists.
- Approved Declaration Records of CIP Exceptional Circumstances (CEC), if any, and supporting documentation where CEC has impacted an ability to comply, and where the provision for CEC exists.
- Any lists or records required by configuration monitoring process(es), including but not limited to records like:
 - Dated detected potential unauthorized baseline deviations, the subject Cyber Asset(s), and the affected baseline attribute(s),
 - Dated alerts of detected potential unauthorized baseline deviations,
 - Dated review or acknowledgement records that alerts were received, assessed, and addressed; and any records that may have been generated to support the activation of Incident Response (if needed),
 - Dated system configurations of which Cyber Assets and which corresponding configuration attributes are monitored, inclusive of the cycle on which the monitoring is set to occur,
 - Dated system configurations of alert log retention intervals, and/or forwarding parameters to send to a centralized SIEM, if any,
 - Dated system configurations to present alerts to a console/display and/or disseminate alerts to responders via alternate methods, and/or
 - Dated authorizations corresponding to detected baseline changes that after investigation did not qualify as unauthorized, and baseline documentation updates.



APPENDIX D: SUPPORTING ANALYSIS; ASSESSING & TESTING

Supporting Analysis – CIP-005 Cybersecurity Controls

The CIP Subject Matter Expert Team has performed an in-depth analysis and offers [Table 1 – CIP-005 Cybersecurity Controls](#) as a potential option for entities as they consider how to design, build, maintain, and/or mature their programs.

*Criteria: Note that the CIP Cyber Security Reliability Standards define the minimum criteria for which impact rated BES Cyber Assets/Systems and associated Cyber Assets are applicable. The below table does not replace nor supersede that mandatory obligation, nor does it increase the scope of qualifying “**Applicable System(s)**” as defined within the Standards. Because this Criterion is already defined and relevant to every Requirement Part, for simplicity the Subject Matter Expert team has not repeated this in the Criteria column of this table.

Table 1 – CIP-005 Cybersecurity Controls

Requirement	Associated Security Control(s)	Criteria*
CIP-005-5, Requirement R1 Part 1.1	<ul style="list-style-type: none"> Logical residence within an Electronic Security Perimeter (ESP) 	<ul style="list-style-type: none"> Network connected, and using a routable protocol.
CIP-005-5 Requirement R1 Part 1.2	<ul style="list-style-type: none"> Inbound & outbound Electronic Access Point (EAP) protection. 	<ul style="list-style-type: none"> Routable traffic traversing ESP.
CIP-005-5 Requirement R1 Part 1.3	<ul style="list-style-type: none"> Configured inbound & outbound access permissions. Reasons that warrant configured access permissions. Denial of access by default. 	<ul style="list-style-type: none"> Routable host traffic traversing ESP. Routable user traffic traversing ESP.
CIP-005-5 Requirement R1 Part 1.4	<ul style="list-style-type: none"> Dial-up authentication. 	<ul style="list-style-type: none"> If dial-up is used. If authentication is Technically Feasible.
CIP-005-5 Requirement R1 Part 1.5	<ul style="list-style-type: none"> Inbound and outbound detective mechanisms for malicious communications. 	<ul style="list-style-type: none"> Where an EAP exists.
CIP-005-5 Requirement R2 Part 2.1	<ul style="list-style-type: none"> Intermediate System functionality preventing direct access. 	<ul style="list-style-type: none"> Where Interactive Remote Access is used.
CIP-005-5 Requirement R2 Part 2.2	<ul style="list-style-type: none"> Encryption functionality between accessing host and the Intermediate system. 	<ul style="list-style-type: none"> Where Interactive Remote Access is used.
CIP-005-5 Requirement R2 Part 2.3	<ul style="list-style-type: none"> Multi-factor authentication functionality into the Intermediate System from the accessing host. 	<ul style="list-style-type: none"> Where Interactive Remote Access is used.



Supporting Analysis – CIP-007 Cybersecurity Controls

The CIP Subject Matter Expert Team has performed an in-depth analysis and offers [Table 2 – CIP-007 Cybersecurity Controls](#) as a potential option for entities as they consider how to design, build, maintain, and/or mature their programs.

*Criteria: Note that the CIP Cyber Security Reliability Standards define the minimum criteria for which impact rated BES Cyber Assets/Systems and associated Cyber Assets are applicable. The below table does not replace nor supersede that mandatory obligation, nor does it increase the scope of qualifying “**Applicable System(s)**” as defined within the Standards. Because this Criterion is already defined and relevant to every Requirement Part, for simplicity the Subject Matter Expert team has not repeated this in the Criteria column of this table.

Table 2 – CIP-007 Cybersecurity Controls

Requirement	Associated Security Control(s)	Criteria*
CIP-007-6 Requirement R1 Part 1.1	<ul style="list-style-type: none"> Disabling of, or restricting controls for, unneeded network accessible logical ports, or port ranges. 	<ul style="list-style-type: none"> Network connected, and Using a routable protocol.
CIP-007-6 Requirement R1 Part 1.2	<ul style="list-style-type: none"> Protections against the use of unneeded physical console ports, physical removable media ports, and/or physical network connectivity ports. 	<ul style="list-style-type: none"> Cyber Assets with unneeded or unused physical ports.
CIP-007-6 Requirement R2 Part 2.1-2.3	<ul style="list-style-type: none"> Security patching level commensurate with known/expected installation or documented mitigated status. 	<ul style="list-style-type: none"> Any Cyber Asset where a Patch Source exists.
CIP-007-6 Requirement R3 Part 3.1-3.3	<ul style="list-style-type: none"> Malicious code deterrence, detection, and/or prevention controls, including the: <ul style="list-style-type: none"> Expected/known signature/pattern installation level, or mitigated status for detected malicious code. Parameters and expected system, client, or application settings needed for the retrieval of signature/pattern updates. 	<ul style="list-style-type: none"> Any Cyber Asset where malware prevention tools are locally installed.
CIP-007-6 Requirement R4 Part 4.1	<ul style="list-style-type: none"> Security event monitoring controls configured to log detected successful logins, detected failed access/login attempts, and detected malicious code. <ul style="list-style-type: none"> Parameters and expected system, client, or application settings needed to allocate sufficient local memory or storage for collection of logs. Parameters and expected system, client, or application settings for the forwarding of logs to receivers of centralized solutions. 	<ul style="list-style-type: none"> Any Cyber Asset that has the capability to log prescribed events.
CIP-007-6 Requirement R4 Part 4.2	<ul style="list-style-type: none"> Security event monitoring controls configured to generate alerts for detected logging failures, and detected malicious code, or other identified events necessitating and alert. 	<ul style="list-style-type: none"> Any Cyber Asset that has the capability to alert on specified detected events.



Table 2 – CIP-007 Cybersecurity Controls (continued)		
Requirement	Associated Security Control(s)	Criteria*
	<ul style="list-style-type: none"> Parameters and expected system, client, or application settings needed for the forwarding of detected events to systems designed to ingest logs and disseminate alerts. 	
CIP-007-6 Requirement R4 Part 4.3	<ul style="list-style-type: none"> Security event logging controls configured to retain logs for at least 90 consecutive calendar days. <ul style="list-style-type: none"> Parameters and expected system, client, or application settings needed to allocate sufficient local memory or storage designed to retain of logs. Parameters and expected system, client, or application settings for the forwarding of logs to receivers of centralized solutions designed to retain logs. 	<ul style="list-style-type: none"> Where Interactive Remote Access is used.
CIP-007-6 Requirement R5 Part 5.1	<ul style="list-style-type: none"> Authentication enforcement mechanisms configured for interactive user access. 	<ul style="list-style-type: none"> Cyber Assets with the capability to enforce authentication: Where enabled local physical ports are used. Where Interactive Remote Access is used.
CIP-007-6 Requirement R5 Part 5.2	<ul style="list-style-type: none"> Account and access control status, including alignment with documented known default, generic, and shared account inventories. 	<ul style="list-style-type: none"> Cyber Assets with known default, generic, and shared accounts.
CIP-007-6 Requirement R5 Part 5.3	<ul style="list-style-type: none"> Account and access control status, including authorization records for shared accounts. <ul style="list-style-type: none"> Expected shared account passwords. 	<ul style="list-style-type: none"> Cyber Assets in use shared accounts.
CIP-007-6 Requirement R5 Part 5.4	<ul style="list-style-type: none"> Account and access control status, including changes of known default passwords. <ul style="list-style-type: none"> Password change capability and any expected parameters or settings intended to mitigate where passwords cannot be changed. 	<ul style="list-style-type: none"> Cyber Assets with known default passwords that can be changed.
CIP-007-6 Requirement R5 Part 5.5	<ul style="list-style-type: none"> Account and access control status, including: <ul style="list-style-type: none"> Implemented password length and complexity. Password length and complexity capabilities. 	<ul style="list-style-type: none"> Cyber Assets with password capability.
CIP-007-6 Requirement R5 Part 5.6	<ul style="list-style-type: none"> Account and access control status, including technical controls configured to enforce password changes for password-only authentication for interactive user access. 	<ul style="list-style-type: none"> Cyber Assets with the capability to enforce authentication:



Requirement	Associated Security Control(s)	Criteria*
		<ul style="list-style-type: none"> • Where enabled local physical ports are used. • Where Interactive Remote Access is used.
CIP-007-6 Requirement R5 Part 5.7	<ul style="list-style-type: none"> • Security event logging controls configured to either apply a limit on unsuccessful login attempts and/or alerting configuration for attempts exceeding defined thresholds. <ul style="list-style-type: none"> ○ Parameters and expected system, client, or application settings needed to apply local rules for limits or thresholds. ○ Parameters and expected system, client, or application settings needed to forward events to receivers of centralized solutions designed to monitor thresholds and alert when exceeded. 	<ul style="list-style-type: none"> • Any Cyber Asset that has the capability to utilize a login limit or threshold.

Supporting Analysis – CIP-005 Cybersecurity Controls Verification

The CIP Subject Matter Expert Team has performed an in-depth analysis and offers [Table 3 – CIP-005 Cybersecurity Controls Verification](#) as a potential option for entities as they consider how to design, build, maintain, and/or mature their programs.

*Options & Suggestions: Note that there are myriad approaches, both manual and/or automated, to verifying Security Controls and the table below is not intended to be a prescriptive nor all-inclusive list. Instead, the Verification Options below offer varied examples that could be used in whole or in part as a potential approach to verify post-change security posture. The intention is to offer several potential approaches as examples that a Registered Entity may find helpful or applicable to their environment, processes, and tools. Similarly, the Potential Evidence Suggestions are an un-exhaustive list intended to provide ideas for Registered Entities. The suggestions do not replace nor supersede the Measures as documented in the Standards and Requirements.

Table 3 – CIP-005 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-005-5, Requirement R1 Part 1.1	<ul style="list-style-type: none"> • Perform a physical walk-down and cable tracing of the connections, making note of wireless capabilities, to each Cyber Asset and compare to the ESP Diagram. • Execute commands locally on each Cyber Asset to verify the configuration of the routable interface and compare to the ESP Diagram. • Perform network-based commands like a ping sweep or traceroute to confirm logical location and compare to the ESP Diagram. 	<ul style="list-style-type: none"> • Updated ESP Diagram illustrating Cyber Asset(s) inside the ESP. • Screenshots or system-generated local output of network interface configurations • Screenshots or system-generated output of network-based commands and Cyber Asset responses. • Screenshots or system-generated output from automated discovery or



Table 3 – CIP-005 Cybersecurity Controls Verification (continued)

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
	<ul style="list-style-type: none"> Use implemented scanning/discovery tools to interrogate each Cyber Asset for its routable interface configuration and compare to ESP Diagram. Use tools to perform wireless discovery, documenting and investigating any detected Cyber Assets or any null results. 	<p>scanning tools, including wireless detection tools.</p> <ul style="list-style-type: none"> Vendor materials that support technical capability, or incapability, of Cyber Assets, including where features like wireless, for example, are or are not available
<p>CIP-005-5 Requirement R1 Part 1.2</p>	<ul style="list-style-type: none"> Perform a physical walk-down and cable tracing of the connections to the Cyber Asset(s) and compare to the ESP Diagram. If allowed by the EAP configuration, perform network-based commands like ping or traceroute to confirm logical location and compare to the ESP Diagram. 	<ul style="list-style-type: none"> Updated ESP Diagram illustrating Cyber Asset(s) does not have connected interfaces that are not identified EAPs. Screenshots or system-generated output of network-based commands and Cyber Asset responses demonstrating access route through an EAP.
<p>CIP-005-5 Requirement R1 Part 1.3</p>	<ul style="list-style-type: none"> Review EAP rules and compare to defined and expected allowable inbound and outbound access, and the reasons for it. Attempt to access the Cyber Asset from known authorized and unauthorized networks, hosts, and/or applications outside the ESP and compare to EAP logs. 	<ul style="list-style-type: none"> Screenshots or system-generated output of relevant EAP rules and corresponding justifications for the rules. Screenshots or system-generated local output of access attempts and responses. Screenshots or system-generated output from EAP logs demonstrating expected “allows” or “deny by default” outcomes.



Table 3 – CIP-005 Cybersecurity Controls Verification (continued)		
Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-005-5 Requirement R1 Part 1.4	<ul style="list-style-type: none"> Dial-up into the Cyber Asset and confirm that the authentication mechanisms are implemented and operating as designed. Verify active TFE coverage for Cyber Assets with dial-up and without authentication capability, and that approved mitigating measures are implemented 	<ul style="list-style-type: none"> Screenshots or system-generated output from dial-up utility on the accessing host. Screenshots or system-generated logs from the dial-up authentication server demonstrating access authentication from dial in connection. Dated TFE approval records, lists of covered Cyber Assets, mitigating measures, and screenshots or system-generated outputs demonstrating implemented mitigations.
CIP-005-5 Requirement R1 Part 1.5	<ul style="list-style-type: none"> Perform a physical walk-down and cable tracing of the connections between the Cyber Assets used to monitor the communication path and the node(s) being providing monitoring data, documenting the ports/interface(s) that are wired to a networking device used to locally tap communications and/or any direct hardware-related taps that may be used. If using a logical mirroring/span monitor port: <ul style="list-style-type: none"> Log into the network device controlling the spanned traffic verify the interface configuration. Execute commands to display interface statistics and confirm traffic is present. 	<ul style="list-style-type: none"> Updated diagram illustrating physical connectivity between the Cyber Asset responsible for monitoring and the end node(s)/communication path being monitored. Screenshots or system-generated output of issued commands and dated/timestamped interface statistics demonstrating logical tap configuration is correct and active. Screenshots or system-generated output of issued commands, logs, and/or application dashboards etc. demonstrating traffic for the identified communication path is present for monitoring. Screenshots or <i>system-generated</i> output of the configuration and status of the Cyber Asset(s) responsible for monitoring network communications demonstrating up-to-date pattern/signature files
	<ul style="list-style-type: none"> Using authorized access, log into the Cyber Asset(s) responsible for monitoring network communications and, depending on the capability of the system: <ul style="list-style-type: none"> View logs and/or application dashboards to confirm traffic for the identified communication path is received. 	<ul style="list-style-type: none"> Screenshots or <i>system-generated</i> output of the configuration and status of the Cyber Asset(s) responsible for monitoring network communications demonstrating received traffic, active status indicators for monitoring ports, services and/or policies, and associated logs.



	<ul style="list-style-type: none"> ○ For signature/pattern-based tools, verify signature/patterns are up-to date ○ For whitelist/rule-based systems review logs to assure active traffic and policies. 	
<p>CIP-005-5 Requirement R2 Part 2.1-2.3</p>	<ul style="list-style-type: none"> ● Review EAP rules containing interactive protocols that could be used for Interactive Remote Access (IRA) and compare to defined and expected allowable inbound routable session capability between Cyber Assets inside the ESP and Cyber Assets outside the ESP. <ul style="list-style-type: none"> ○ Review and confirm source node(s) are declared Intermediate Systems (IS). ○ Using authorized access, log into each IS and verify it is configured to encrypt sessions between the IS and the Cyber Asset used for IRA. ○ Review account configuration and authentication mechanisms used by each IS and verify it is multi factor. ● While monitoring EAP communication events and/or authentication server/Intermediate System logs, execute a series of 'login tests' to simulate a user session using the Intermediate System vs a user attempting to use IRA direct, capturing the output of those attempts, including system prompts/access accept or denial messages/errors and associated logs. 	<ul style="list-style-type: none"> ● Screenshots or system-generated output of relevant EAP rules and corresponding justifications for the rules. ● Screenshots or system-generated logs of access attempts and responses, and/or any prompts to authenticate. ● Screenshots or system-generated configuration settings from the Intermediate System demonstrating encryption. ● Screenshots or system-generated configuration settings from the authentication source demonstrating multi-factor access authentication from an Intermediate System. ● Screenshots or <i>system</i>-generated output from EAP (or authentication server) logs demonstrating expected "allows" from Intermediate Systems or "deny" for attempted direct IRA.

Supporting Analysis – CIP-007 Cybersecurity Controls Verification

The CIP Subject Matter Expert Team has performed an in-depth analysis and offers [Table 4 – CIP-007 Cybersecurity Controls Verification](#) as a potential option for entities as they consider how to design, build, maintain, and/or mature their programs.

*Options & Suggestions: Note that there are myriad approaches, both manual and/or automated, to verifying Security Controls and the table below is not intended to be a prescriptive nor all-inclusive list. Instead, the Verification Options below offer varied examples that could be used in whole or in part as a potential approach to verify post-change security posture. The intention is to offer several potential approaches as examples that a Registered Entity may find helpful or applicable to their environment, processes, and tools. Similarly, the Potential Evidence Suggestions are an un-exhaustive list intended to provide ideas for Registered Entities. The suggestions do not replace nor supersede the Measures as documented in the Standards and Requirements.



Table 4 – CIP-007 Cybersecurity Controls Verification		
Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-007-6 Requirement R1 Part 1.1	<ul style="list-style-type: none"> Execute commands locally on each Cyber Asset to verify the configuration of network accessible logical ports and compare to established baselines. Review host-based firewall configuration (if any) for network accessible logical ports and compare to established baselines. Use implemented scanning/discovery tools to interrogate each Cyber Asset for its network accessible logical ports and compare to established baselines. 	<ul style="list-style-type: none"> Approved versions of established baselines for network accessible logical ports Screenshots or system-generated local output of logical port configurations or host-based firewall rules. Screenshots or system-generated output of network-based commands and Cyber Asset responses. Screenshots or system-generated output from automated discovery or scanning tools and Cyber Asset responses demonstrating logical port accessibility and status.
CIP-007-6 Requirement R1 Part 1.2	<ul style="list-style-type: none"> Implement physical mechanisms (i.e. port blocking devices, tamper tape etc.) on unused ports and port locking devices on used ports. Perform a physical walk-down to verify physical mechanisms remain in place. Logically disable unused ports within the Cyber Asset interface configuration. Using authorized access, login to the Cyber Asset(s) to verify the unused interfaces remain disabled. 	<ul style="list-style-type: none"> Photographs demonstrating physical mechanisms are in place. Logs from administrative processes documenting unique IDs or serial numbers from physical mechanisms and the date each was removed/replaced for authorized purposes. Screenshots or system-generated outputs of interface commands or configuration settings demonstrating unused physical ports are logically disabled.



Table 4 – CIP-007 Cybersecurity Controls Verification		
Requirement	Security Control(s) Verification <u>Options</u>*	Potential Evidence Suggestions*
CIP-007-6 Requirement R2 Part 2.3-2.4	<p>Compare the output of any tools, reports, and/or commands to security patch applicability assessments and established baselines to assure the expected patch level is installed. (Accommodating, of course, for any conditions where the baseline change was to install security patches that may not be represented in the baseline yet).</p> <p>Potential verification mechanisms like, but not limited to the below could be performed:</p> <ul style="list-style-type: none"> Using authorized access, connect to the Cyber Asset(s) locally or through IRA and view system configuration, registry, and/or execute commands that display currently installed patches. Compare the output of these tools/commands to security patch applicability assessments and established baselines to assure the expected patch level is installed. Using authorized access, connect to a centralized patch management system and view the system configuration, and/or registry of the Cyber Asset(s) for currently installed patches. Using an authorized querying tool designed to interrogate for security patch level, retrieve the status of installed security patches for the Cyber Asset(s). Using a preconfigured reporting system that communicates with a security patch inventory system configured to retrieve actual status, generate an on-demand report of the installed security patches for the Cyber Asset(s). 	<ul style="list-style-type: none"> Approved versions of established baselines for applied security patches. Security patch applicability assessment records. Vendor release notes for pertinent security patches. Screenshots, reports, or system-generated output of system configuration, registry, and/or any executed commands and Cyber Asset responses displaying security patch level. Security testing documentation that records the comparison results. Documentation of any variances from expected results and associated mitigating, corrective, or rollback actions including the status of said actions.



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
<p>CIP-007-6 Requirement R3 Part 3.1-3.3</p>	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA and view system configuration, registry, and/or execute commands that display malicious software prevention tools and status. Verify the software is installed, running, has configured scan cycles and triggers per Registered Entity setup procedures, and that signature/pattern installation level is up-to-date. • Using authorized access, connect to a centralized malware prevention system and view the system configuration of the Cyber Asset(s). Verify the software is installed, running, has configured scan cycles and triggers per Registered Entity setup procedures, and that signature/pattern installation level is up-to-date. 	<ul style="list-style-type: none"> • Documented setup procedures for malware prevention software detailing expected client configuration for scanning cycles/triggers and periodicity for signature/pattern updates. • Screenshots or system-generated output of issued commands, logs, and/or application dashboards etc. demonstrating malware preventions software is installed and running. • Screenshots or system-generated output of the configuration and status of the Cyber Asset(s) demonstrating up-to-date pattern/signature files.
<p>CIP-007-6 Requirement R4 Part 4.1</p>	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the logging and alerting controls for security events. • View system configuration, and/or execute commands that return settings: <ul style="list-style-type: none"> ○ to control detection of successful and failed login attempts. Verify local logging settings include these security events. ○ to control detection of malicious code. Verify the malware prevention software is installed, running, has configured scan cycles and triggers per Registered Entity setup procedures, and that signature/pattern installation level is up-to-date. ○ that define forwarding to a centralized receiver, if any. Verify settings. 	<ul style="list-style-type: none"> • Documented setup procedures for security event configuration detailing expected local/client configuration and/or forwarding parameters for centralized receivers. • Screenshots or system-generated output of parameters that depict the Cyber Asset’s system, client, or application settings that identify security events to log (demonstrates event detection and logging capability). • Screenshots or system-generated output of logs containing both successful and failed logins (demonstrates event detection and logging). • Screenshots or <i>system-generated</i> output of malware prevention software logs containing simulated malicious code (demonstrates event detection and logging).



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification <u>Options*</u>	Potential Evidence Suggestions*
<p>CIP-007-6 Requirement R4 Part 4.1 (continued)</p>	<p>Examples:</p> <ul style="list-style-type: none"> ○ Confirm the Cyber Asset’s IP interface and default gateway configuration. ○ Confirm the IP of the centralized receiver is properly identified in the system, application, or logging client, service, or daemon configuration. <ul style="list-style-type: none"> ● Generate a successful login and view the local log file to confirm the event was detected and logged. Connect to any centralized receiver and confirm the logged event was forwarded/ingested. ● Generate an intentional failed login and view the local log file as to confirm event was detected and logged. Connect to any centralized receiver and confirm the logged event was forwarded/ingested. ● Use a tool (i.e. Bitdefender/Eicar etc.) to simulate malware and view the client logs to confirm the event was detected and logged. Connect to any centralized receiver and confirm the logged event was forwarded/ingested. 	<ul style="list-style-type: none"> ● Screenshots or <i>system-generated</i> output of the configuration and status of the Cyber Asset(s) (demonstrating up-to-date pattern/signature files to support detection capability.)
<p>CIP-007-6 Requirement R4 Part 4.2</p>	<ul style="list-style-type: none"> ● Generate an intentional failed login to the Cyber Asset locally or through IRA and: <ul style="list-style-type: none"> ○ View the failed login event monitoring display/dashboard (could be a log file) to confirm the event was detected. ○ Connect to the centralized receiver, if any, and confirm the detected event was forwarded/ingested and displays the monitoring view/dashboard. ○ Access alerting tools and verify the event generated an alert and it was received as expected. ● Use an authorized tool (i.e. Bitdefender/Eicar etc.) to simulate malware on the Cyber Asset and: 	<ul style="list-style-type: none"> ● Approved versions of documented setup procedures for security event detection, monitoring, and the tools used to receive alerts (i.e. email, text message, on call queue, alarm monitor display etc.). ● Screenshots or system-generated output of monitoring display/dashboard containing both failed logins and simulated malicious code (demonstrates event are detection). ● Screenshots or copies of received alerts for failed logins and detected malware (demonstrates expected alerts are generated and received for tested events).



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
<p>CIP-007-6 Requirement R4 Part 4.2 (continued)</p>	<ul style="list-style-type: none"> ○ View malware monitoring display/dashboard (could be a log file) to confirm the event was detected. ○ Connect to the centralized receiver, if any, and confirm the detected event was forwarded/ingested and displays the monitoring view/dashboard. ○ Access alerting tools and verify the event generated an alert that was received as expected. 	
<p>CIP-007-6 Requirement R4 Part 4.3</p>	<ul style="list-style-type: none"> ● Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the log retention controls for detected security events. ● View system configuration, and/or execute commands that return settings: <ul style="list-style-type: none"> ○ That allocate local memory or disk for log retention. ○ That specify retention interval of 90 calendar days. ○ That automate local archival from the log to a file on a rolling interval that assures 90 calendar days of logs. ○ That define forwarding to a centralized receiver, if any, for retention. ● Connect to the centralized receiver, if any, and view system configuration, and/or execute commands that return settings: <ul style="list-style-type: none"> ○ That allocate local memory or disk for log retention. ○ That specify retention interval of 90 calendar days. 	<ul style="list-style-type: none"> ● Approved versions of documented setup procedures for security log retention intervals and repositories. ● Screenshots or system-generated output of configured parameters that control log retention intervals for local or centralized repositories. ● Screenshots or copies of received alerts for failed logins and detected malware (demonstrates expected alerts are generated and received for tested events).



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
<p>CIP-007-6 Requirement R5 Part 5.1</p>	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the configured authentication enforcement mechanisms. • View system configuration, and/or execute commands that return settings: <ul style="list-style-type: none"> ○ For each enabled 1) locally accessible physical input/output (I/O) port capable of user access, 2) locally accessible accounts, and 3) remotely accessible accounts, if any and: <ul style="list-style-type: none"> ▪ Verify enforcement of authentication is enabled for each account/interface, either locally or through the configuration of a remote authentication server. ▪ Verify active TFE coverage for Cyber Assets without capability, and that approved mitigating measures are implemented. • Resolve identified discrepancies, if any, by: <ul style="list-style-type: none"> ○ Adjusting Cyber Asset settings to align configuration with approved expected enforcement status, and/or ○ Executing the process to obtain TFE coverage. 	<ul style="list-style-type: none"> • Approved versions of documented setup procedures for authentication enforcement mechanisms and configuration parameters. • Documented list of expected and authorized accounts and/or I/O ports. • Screenshots or <i>system-generated</i> output of Cyber Asset accounts and associated status. • Screenshots or <i>system-generated</i> output of I/O ports capable if interactive user access accounts and associated status. • Screenshots or <i>system-generated</i> output of configured parameters that enforce authentication for each enabled account/physical I/O port. • Dated TFE approval records, lists of covered Cyber Assets, mitigating measures, and screenshots or <i>system-generated</i> outputs demonstrating implemented mitigations. • Documented variances between account inventory and account setup, if any. • <i>System-generated</i> output of end state for Cyber Asset authentication enforcement or TFE coverage request/approval records (demonstrates variances were addressed).
<p>CIP-007-6 Requirement R5 Part 5.2</p>	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the configured accounts. • View system configuration, and/or execute commands that return status of each known default or otherwise generic accounts. • Compare to documented account inventory and verify alignment actual status. • Resolve identified discrepancies, if any, by: 	<ul style="list-style-type: none"> • Approved versions of documented account inventory for default or otherwise generic accounts. • Screenshots or <i>system-generated</i> output of Cyber Asset default or otherwise generic accounts and associated status. • Documented variances between account inventory and account setup, if any. • Screenshots or <i>system-generated</i> output of end state for Cyber Asset default or otherwise generic accounts following



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-007-6 Requirement R5 Part 5.2 (continued)	<ul style="list-style-type: none"> ○ Adjusting Cyber Asset settings to align configuration with approved account inventory and expected status, and/or ○ Executing the approval process to update the account inventory and expected status to align with new configuration. 	actions to resolve identified variances, if any (demonstrates approved configuration matches actual configuration).
CIP-007-6 Requirement R5 Part 5.3	<ul style="list-style-type: none"> ● Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the shared accounts, if any. ● View system configuration, and/or execute commands that return status of each shared account. ● Compare to access management process/system and verify a mechanism exists to authorize users for access to any shared accounts and associated password, and that a list of authorized users aligns with actual access. ● Resolve identified discrepancies, if any, by: ● Adjusting Cyber Asset shared account configuration (potentially changing password) to align with approved account inventory and authorized users, and/or ● Executing the approval process to update the shared account inventory and authorized users to align with new shared account configuration. 	<ul style="list-style-type: none"> ● Approved versions access management process for authorization to shared accounts mechanisms and configuration parameters. ● Documented list of expected shared accounts and users. ● Screenshots or <i>system-generated</i> output of authorization records for shared accounts. ● Screenshots or <i>system-generated</i> output of actual shared accounts and associated status. ● Documented variances between shared account authorizations and account access, if any, and actions to resolve. ● <i>System-generated</i> output of end state for Cyber Asset shared accounts, inclusive of log entries or commands for any password changes that may have been needed to limit access to authorized users (demonstrates variances were addressed).
CIP-007-6 Requirement R5 Part 5.4	<ul style="list-style-type: none"> ● Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the shared accounts, if any. ● View system configuration, and/or execute commands that return status of each account, command line interface, or interactive service (i.e. SNMP) with a known default password. 	<ul style="list-style-type: none"> ● Dated vendor materials identifying limitations with per Cyber Asset capability. ● Screenshots or <i>system-generated</i> output of manual default password testing results. Could include log events demonstrating failed login. ● Screenshots or <i>system-generated</i> output of password change events for default accounts.



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-007-6 Requirement R5 Part 5.4 (continued)	<ul style="list-style-type: none"> • Verify non-default passwords are applied, per Cyber Asset capability by: <ul style="list-style-type: none"> ○ Testing login with the known default password and verifying it fails. Perform manually or with tools designed to do this. (Note: if using a tool assure it contains the relevant default accounts and passwords in its test library). • For newly implemented devices, or detected variances, changing the password to a non-default that meets length and complexity obligations. 	<ul style="list-style-type: none"> • <i>System-generated</i> output of tools used to perform default password testing results, including the tool library including relevant default accounts and passwords. Could include log events demonstrating failed login Screenshots or <i>system-generated</i> output of default password testing results. Could include log events demonstrating failed login.
CIP-007-6 Requirement R5 Part 5.5	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the shared accounts, if any. • View system configuration, and/or execute commands that return status of each account, command line interface, or interactive service (SNMP) that uses password-only authentication and is capable of interactive user access. <ul style="list-style-type: none"> ○ Where the Cyber Asset has technical features to enforce password complexity and the capability exists: <ul style="list-style-type: none"> ▪ Verify settings to control password length are set to 8 characters minimum. ▪ Verify setting to control password composition are configured to require at least three different types of characters. ○ Where the Cyber Asset capability has technical features to enforce password complexity but does not support the minimum length and composition: 	<ul style="list-style-type: none"> • Approved versions of documented operating procedures including administrative mechanisms used to procedurally enforce password complexity for password-only authentication associated to interactive user access capability. • Approved versions of documented setup procedures including technical parameters configured to achieve automated enforcement for password complexity. • Screenshots or <i>system-generated</i> output of password complexity enforcement settings for length and character composition. • Vendor materials to support instances where per Cyber Asset capability precludes conformance with: <ul style="list-style-type: none"> • 8-character length. • 3-character composition. • Technical enforcement of complexity parameter(s) • Dated TFE approval records, lists of covered Cyber Assets, mitigating measures, and screenshots or <i>system-generated</i> outputs demonstrating implemented mitigations



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification Options*	Potential Evidence Suggestions*
CIP-007-6 Requirement R5 Part 5.5 (continued)	<ul style="list-style-type: none"> ▪ Verify settings to control password length are set to align with the maximum per Cyber Asset capability. ▪ Verify setting to control password composition are to align with the maximum per Cyber Asset capability. • Where the Cyber Asset does not have technical features to enforce password complexity (length or composition), verify active TFE coverage for Cyber Assets without password change capability, and that approved mitigating measures are implemented. 	<ul style="list-style-type: none"> • Documented variances between password complexity enforcement setup, if any. • <i>System-generated</i> output of end state for Cyber Asset password complexity enforcement setup or TFE coverage request/approval records (demonstrates variances were addressed).
CIP-007-6 Requirement R5 Part 5.6	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) locally or through IRA to verify the password status. • View system configuration, and/or execute commands that return settings: <ul style="list-style-type: none"> ○ For configured enforcement mechanisms for each password: <ul style="list-style-type: none"> ▪ Where password change enforcement is achieved procedurally, verify for each account, command line interface, or interactive service (i.e. SNMP), that a password is applied and has been changed within the past 15 months ▪ Where password change enforcement can be achieved technically, verify parameters are set to auto-expire passwords, force password changes, and/or disable associated account, command line interface, or interactive service on an interval not to exceed 15 calendar months 	<ul style="list-style-type: none"> • Approved versions of documented operating procedures including administrative mechanisms used to procedurally enforce password changes once every 15 calendar months. • Approved versions of documented setup procedures including technical parameters configured to achieve automated password change enforcement. • Screenshots or <i>system-generated</i> output of configured parameters that technically enforce password change. • Screenshots or <i>system-generated</i> output of event logs containing evidence of password change actions and dates. • Dated TFE approval records, lists of covered Cyber Assets, mitigating measures, and screenshots or <i>system-generated</i> outputs demonstrating implemented mitigations. • Documented variances between password change enforcement capability and setup, if any (demonstrates variances were addressed).



Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification <u>Options</u> *	Potential Evidence Suggestions*
CIP-007-6 Requirement R5 Part 5.6 (continued)	<ul style="list-style-type: none"> ▪ Where password change enforcement cannot be achieved technically, verify active TFE coverage for Cyber Assets without password change capability, and that approved mitigating measures are implemented. • Resolve identified discrepancies, if any, by: <ul style="list-style-type: none"> ○ Configuring password change enforcement parameters and enabling automated mechanisms to technically enforce. ○ Manually changing passwords on the Cyber Asset if procedural enforcement is the only mechanism available, and/or • Executing the process to obtain TFE coverage. 	<ul style="list-style-type: none"> • <i>System-generated</i> output of end state for Cyber Asset authentication enforcement or TFE coverage request/approval records.
CIP-007-6 Requirement R5 Part 5.7	<ul style="list-style-type: none"> • Using authorized access, connect to the Cyber Asset(s) and verify expected limits or thresholds are set for unauthorized access attempts. <ul style="list-style-type: none"> ○ Verify parameters/setting that identify limits or thresholds for unauthorized access attempts are set. ○ Verify parameters/setting that act to disable, timeout, lock out, or otherwise prevent interactive user access are configured to trigger upon limit or threshold exceedances for unauthorized access attempts are set ○ Verify parameters/settings that control alerting for exceedance of limits or thresholds for unauthorized access attempts are set. • Intentionally fail consecutive logins in excess of set limit/threshold to test account disablement and alerting mechanisms. 	<ul style="list-style-type: none"> • Approved versions of documented setup procedures for security event thresholds or limits on failed logins. • Screenshots or <i>system-generated</i> output of configured parameters that control event thresholds or limits for failed logins. • Screenshots or <i>system-generated</i> output of configured parameters that act to prevent interactive user access upon exceedance of thresholds or limits for failed logins. • Screenshots or <i>system-generated</i> output of configured parameters that generate alerts upon exceedance of thresholds or limits for failed logins. • Screenshots or copies of received failed logins alerts for exceeding threshold for unauthorized attempts (demonstrates expected alerts are generated and received for tested events).

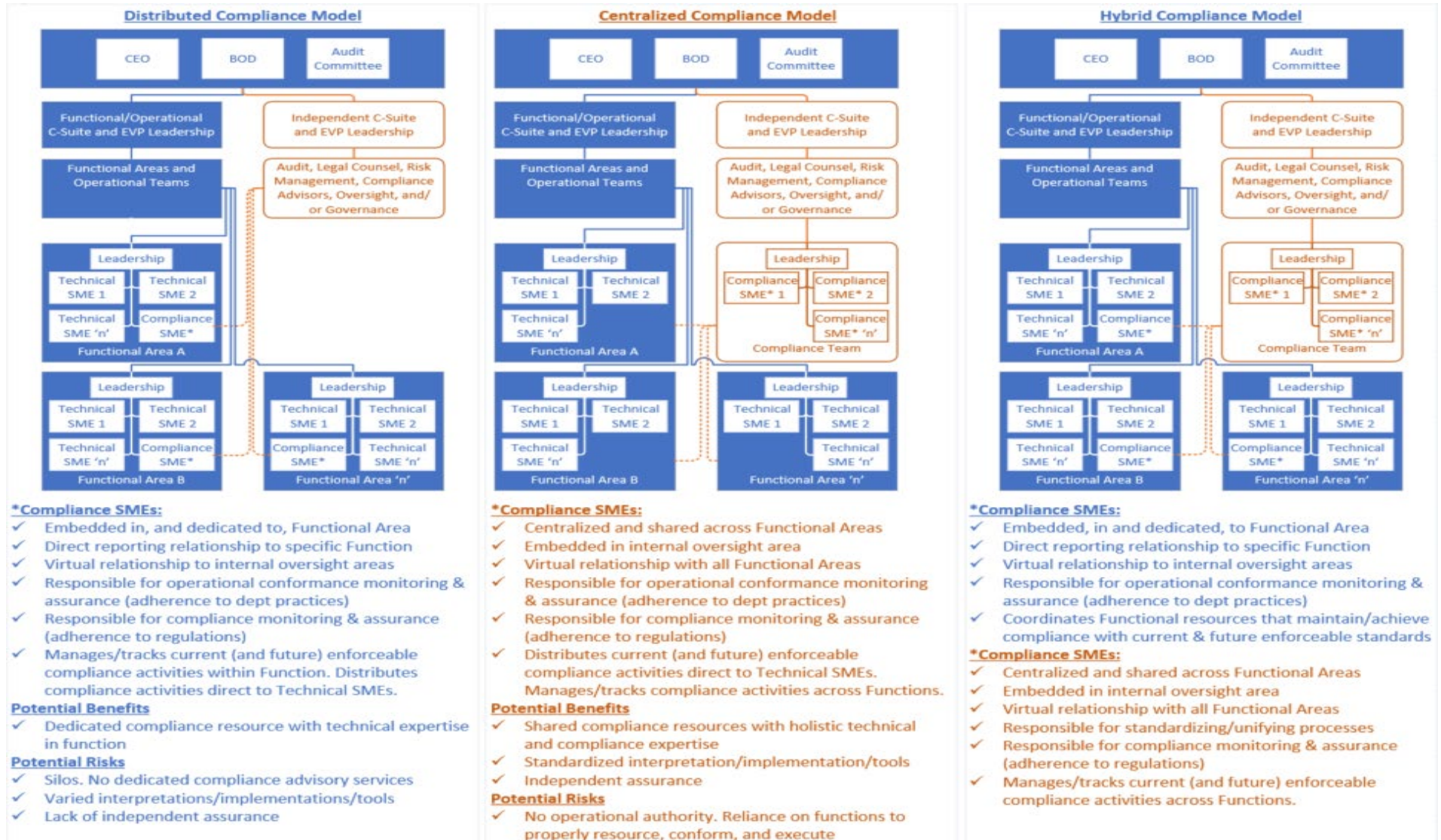


Table 4 – CIP-007 Cybersecurity Controls Verification

Requirement	Security Control(s) Verification <u>Options</u> *	Potential Evidence Suggestions*
CIP-007-6 Requirement R5 Part 5.7 (continued)	<ul style="list-style-type: none"> • Validate the interactive user access is no longer operable after the limit/ threshold is exceeded, or • Verify the expected alert for exceedance of limit/threshold is received after the limit/ threshold is exceeded. • Where the setting of limits, thresholds, and/or automated actions to disable interactive user access or alert on exceedances cannot be achieved technically, verify active TFE coverage for Cyber Assets, and that approved mitigating measures are implemented. • Resolve identified discrepancies, if any, by: • Configuring limits/threshold parameters and enabling automated mechanisms to disable interactive user access or alert upon exceedances, or • Executing the process to obtain TFE coverage. 	<ul style="list-style-type: none"> • Dated TFE approval records, lists of covered Cyber Assets, mitigating measures, and screenshots or <i>system-generated</i> outputs demonstrating implemented mitigations. • Documented variances between limit/threshold and disablement/alerting actions and setup, if any (demonstrates variances were addressed). • <i>System-generated</i> output of end state for Cyber Asset authentication enforcement or TFE coverage request/approval records.



APPENDIX E - GOVERNANCE, SELF-MONITORING, & REASONABLE ASSURANCE OPTIONS



Control Types:

Several concepts exist for designing internal controls to mitigate risk. General terminology like primary, secondary and tertiary controls is sometimes used. Another concept is Key and Non-Key controls. These terms are similar with nuance. In general terms, the distinction is as follows:

- Primary, secondary, and tertiary is often used to identify the relationship between distinct controls. These are often layered safeguards where one monitors the health of another in the spirit of assuring primary control remains operational, and when it fails there is timely visibility into that failure.
- Key and Non-Key are little different in concept in that they share a common objective and risk. Key controls are the primary control relied upon to meet the common objective and mitigate the risk. The spirit of a Non-Key control is to serve as an alternative (or backup) control that still accomplishes the same objective and mitigates the same risk. This differs from the spirit of a secondary control.

Additionally, some of these operational control samples are manual (or administrative) controls while others are automated (or technical) controls. It is also possible to have hybrid controls (technology dependent administrative controls) that have both automated and manual components when executed. For example, an autogenerated report that is automatically distributed via email to a person(s) responsible for a manual review. In the absence of the technological automation there is no source to review, and in the absence of the person the report alone does not mitigate the risk; both components are needed for the control to operate as designed.

Approach:

In each section of this SAG, the CIP SME Team identified operational control samples to mitigate a specific operational or security risk that if left unmitigated could lead to non-compliance. These controls samples are a collection of primary, secondary, and tertiary as well as Key and Non-Key controls.

Each affected functional area may serve a specific business function and be subject to different types or levels of risk. Some may be responsible for cross-functional or enterprise controls that may have a more pervasive impact if not operating as designed. As a result, the tools or mechanisms employed to mitigate those risks may require varied levels of rigor, resources, and/or automation to be effective. Additionally, conditions may exist where secondary or tertiary controls serve to detect when the primary control may not be operating as designed, offering the Registered Entity margin before a condition reaches the level of non-compliance. Each functional area may want to consider establishing an inventory of its operational controls that links to an inventory of operational risks (or risk registry). This operational risk registry can later be used to identify dependencies or cross-functional risks.

The approach to follow leverages the Three Lines of Defense model¹⁷, from the Institute of Internal Audit. In the Three Lines of Defense model operational management control is the first line of defense in risk management; the various risk control and compliance oversight functions established by management are the second line of defense; independent assurance is the third.

¹⁷ <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>



Three Lines of Defense	
1 st Line of Defense	A Registered Entity's first line of defense is each operational area responsible for day-to-day key control activities for configuration change management and monitoring performed by the SMEs. In each guidance section we refer to these internal control measures (or management practices) as "Operational Control Samples".
2 nd Line of Defense	A second line of defense is a Registered Entity's oversight and governance programs that self-assess conformance to documented practices, supervise or monitor of the functional area's execution of internal controls, and oversee and track risk mitigation activities related to security and non-compliance with CIP Cyber Security Reliability Standard Requirements. Programs that serve in this capacity include, but may not be limited to, <ul style="list-style-type: none"> • Compliance, • Enterprise Risk Management (ERM), • Governance, Risk, & Controls (GRC), • Center of Excellence (CoE)
3 rd Line of Defense	A third line of defense is independent and reasonable assurance. Registered Entities may also want to consider extending their internal controls program to provide this level of assurance. <ul style="list-style-type: none"> • One approach could be to engage resources from Internal Audit (IA) to design and operationalize a risk-based assurance program for internal controls related to security inclusive of the CIP Cyber Security Reliability Standard Requirements. By partnering with Internal Audit, these experts can establish test plans to sample records and verify the design effectiveness of internal controls, giving a Registered Entity an auditor's perspective before the CEA executes monitoring and oversight activities. • Another approach could be to engage a completely independent external consulting organization that specializes in auditing, internal controls, and assurance functions.

While external consulting resources may provide a straight forward line of independence for assurance audits, Registered Entities may want to consider the value proposition of choosing to partner with internal resources/programs. Where a model like the three lines of defense is leveraged, strong segregated duties and independent reporting to the CEO, Audit Committee, and Board of Directors can provide opportunities for a functional-area-independent evaluation of the design and sufficiency of internal controls and self-assessment practices. Additionally, personnel trained in compliance, audit, and risk management may also offer a perspective that could otherwise go un-realized by the operational area that executes CIP-related tasks. This method can provide these benefits:



- Establishing a centralized Risk Control Matrix (RCM) that inventories operational and global internal controls, objectives, and risks across the enterprise.
- Facilitating linkage of internal controls and operational risks to an enterprise risk registry thereby offering a holistic view of the Registered Entity's risks and mitigation activities that can be aligned to (and provide support for) a Registered Entity's corporate mission, vision, business objectives, strategies, and values.
- Opening the opportunity for additional internal governance functions for self-assessments and/or an independent internal control testing program thereby providing a mechanism to routinely assess if operational controls are effectively designed.
- Serving as a preparedness activity for NERC CMEP activities like external audits or self-certifications and other oversight activities by the regional CEA. Ongoing oversight readiness and a culture of self-monitoring and improvement. It can garner trust, foster confidence and transparency, and may help calm any natural anxiety that SMEs sometimes experience when preparing for an external audit.

Registered Entities are encouraged to identify, rank, and document risks. Risk is also not limited to compliance risk; risk comes in many forms including reliability risk, security risk, reputational risk etc. Internal controls should be designed to mitigate risk, and established schedules to periodically test a sample of the internal controls should be commensurate with risk. Where testing occurs, personnel trained in audit can partner with functional teams to establish test plans and cycles that provide reasonable assurance that internal controls are effectively designed and operating as intended.

Registered Entities that leverage the three lines of defense are employing methodologies with layered safeguards, and while not synonymous, modelling a defense in depth type strategy to prevent perfect storm through coordinated use of multiple countermeasures to protect the operability of controls that preserve the availability, confidentiality, and integrity of the information and Cyber Assets needed to assure safe, secure, reliable, and resilient operation of the Bulk Electric System.

Internal Controls Design:

One approach that can be helpful is to establish a Risk Statement and Control Objective prior to designing the internal control. This helps assure the control activity is focused on the right thing; mitigating risk by meeting the objective.

Next, internal controls must be measurable to repeatedly perform them and to effectively test them. When constructing internal controls, Registered Entities may want to consider leveraging a standardized framework/model to provide a consistent format inclusive of any necessary information to make it measurable.

Using a tool like FRASA helps to assure inclusion of common details that an Internal Control Activity Statement should be comprised of and can be a good starting point to help SMEs construct internal controls if they are unfamiliar with the concept. In this approach, FRASA stands for the following:

- **Frequency:** The periodicity or cycle on which the activity is performed
- **Responsible Party:** Who is performing the activity (role, job title, function, or named person)
- **Activity:** The specific risk mitigating check or task that is being performed
- **Source:** Where the information is coming from
- **Action Taken:** Action performed in response to observations or discoveries from the activity.

The following examples illustrate the use of a Risk Statement and Control Objective combined with the FRASA tool to develop primary, secondary and tertiary controls to mitigate the risk of potential adverse security-related conditions and consequences from non-compliance with CIP-010-2 Requirement R2 Part



2.1. Registered Entities are not required to implement three levels of controls to achieve and maintain compliance; however, this section is being provided to demonstrate how this approach can be implemented over time to build rigor into a program, continuously improve and further mitigate security, reliability, and compliance risk.



Example A: Primary Control (Key Control)

Internal Control to Mitigate Security & Reliability Risk, and Maintain Compliance

Risk Statement: Unauthorized configuration baseline changes result in compromise of BES Cyber Systems and/or applicable Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES), concurrently causing non-compliance with mandatory regulatory obligations.

Control Objective: Detect and remediate any unapproved configuration baseline changes to reduce the risk of compromise of BES Cyber Systems and/or applicable Cyber Systems, while also maintaining compliance with mandatory regulatory obligations.

Control Activity Attributes:

Frequency:	Every 7 calendar days
Responsible Party:	On-call EMS Administrator
Activity:	Generates the “EMS BCA - Detected Baseline Configuration Changes” report and compares entries to the dashboard of approved EMS BCA changes. Results are documented in an “Unauthorized Baseline Change Review Record” that is saved to the CIP-010-2 R2.1 Evidence Repository, even if results are null.
Source(s): ¹⁸	1. Baseline Monitoring Tool 2. Change Control Ticketing System
Action Taken	Identified variances are researched, reconciled in accordance with change control processes and timelines, and reported by the end of the next business day to the compliance team and senior management for inclusion in corrective action program to mitigate the risk of recurrence and assure any mandatory regulatory reporting obligations are met.

Control Activity Statement: On a cycle of once per 7 calendar days, the on-call EMS Administrator, using the Baseline Monitoring Tool, generates the “EMS BCA - Detected Baseline Configuration Changes” report and compares entries to the dashboard of approved EMS BCA changes within the Change Control Ticketing System and documents the results in an “Unauthorized Baseline Change Review Record” that is saved to the CIP-010-2 R2.1 Evidence Repository, even if results are null. Identified variances are researched, reconciled in accordance with change control processes and timelines, and reported by the end of the next business day to the compliance team and senior management for inclusion in corrective action program to mitigate the risk of recurrence and assure any mandatory regulatory reporting obligations are met.

Note: The Registered Entity that designed this primary control implemented a frequency different than the minimum timeframe of CIP-010-2 Requirement R2 Part 2.1, which mandates a minimum monitoring interval of “at least once every 35 calendar days”. There could be many reasons why this entity has decided upon that interval, like but not limited to:

¹⁸ Note: When identifying the source, typically any tools or technology is referred to by application and vendor name. For the purposes of keeping this guide vendor agnostic, generic references have been used to describe the source.



- Perhaps this entity did not have a repeatable way to manage a rolling 35 calendar day cycle, and routinely missed that mandatory monitoring timeframe leading to self-reports of non-compliance and increased compliance risk beyond the entity's tolerance. Maybe a natural weekly milestone added the repeatability needed for success.
- Perhaps the entity's on-call schedule changes every 7 calendar days and this task is the first thing the on-call person performs during weekly turnover of these duties thereby providing operational consistency and opportunity for continuity of work.
- Perhaps the entity used to monitor every 35 calendar days and detected so many high-risk variances that is exceeded management's risk tolerance and internal controls changed to align with more rigorous cybersecurity best practices to further minimize risk.
- Perhaps the process is new, and the entity is performing this activity more routinely to assure personnel are adequately trained on the monitoring process, and to assure personnel responsible for configuration change are deterred from obviating the process.
- Perhaps the number of EMS BCAs or the volume of change is so significant that the entity must perform the task more frequently to effectively manage the workload of a manual comparison.
- Perhaps the entity used to monitor manually every 35 calendar days now has tools that are now capable of more sophisticated or automated reporting and this has facilitated maturity of the processes and controls.

Regardless of the reason, Registered Entities should be cognizant of variables like these and are encouraged to leverage these examples as considerations to define the depth and breadth of internal controls. Registered Entities can tailor an internal controls program to the organizations' resources, culture, priorities, risk tolerance, and unique environment and resources while achieving and maintaining compliance.

Full reliance on one primary control may not provide a risk-adverse organization with enough assurance that the BES Cyber System is secure and that compliance with mandatory regulatory obligations is met and will be maintained. The next examples illustrate a secondary control that can help answer the question, "How do I know the primary control is working and delivering the expected results?"

Note: An example RCM is also provided following the primary, secondary, and tertiary controls examples. This RCM depicts some additional examples of more automated secondary and tertiary controls that can also add rigor to a Registered Entity's internal controls program.



Example B: Secondary Control

Internal Control for Process Conformance and Compliance Sufficiency Review

Risk Statement: The primary control for monitoring, detection, review, and reconciliation of unauthorized configuration baseline changes is not being performed, or is not operating as designed, resulting in compromise of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).

Control Objective: Verify execution of primary control conforms with expected cycles, actions, and results documentation.

Control Activity Attributes:

Frequency:	The first business day of each calendar month
Responsible Party:	Reliability Standards Compliance Analyst
Activity:	Verifies a “Baseline Configuration Change Review Record” exists for each week in the previous calendar month, and that each record includes documented results of the expected comparison, any identified variances, and associated remediation actions, even if results are null.
Source(s):	CIP-010-2 R2.1 Evidence Repository
Action Taken	Identified missing or incomplete records, associated details, and risks of impending non-compliance with the 35 calendar day requirement are documented, added to the monthly conformance monitoring report, and distributed within 3 calendar days to the compliance team and senior management for risk assessment remediation within compliance timeframes.

Control Activity Statement: On first business day of each calendar month, the EMS Compliance Coordinator, using authorized read-only access to the CIP-010-2 R2.1 Evidence Repository, verifies a “Baseline Configuration Change Review Record” exists for each week in the previous calendar month, and that each record includes documented results of the expected comparison, any identified variances, and associated remediation actions, even if results are null. Identified missing or incomplete records, associated details, and risks of impending non-compliance with the 35 calendar day requirement are documented, added to the monthly conformance monitoring report, and distributed within 3 calendar days to the compliance team and senior management for risk assessment remediation within compliance timeframes.

While this secondary control provides additional confidence that the primary control is working, each Registered Entity must define its risk appetite. Tertiary self-monitoring controls are sometimes referred to as a Test Plan or an Assurance Audit and are used to test the design effectiveness and conformance to primary or secondary controls. The next examples illustrate a secondary control that can help answer the question,

“How can I be assured that primary and secondary internal controls are effectively designed to mitigate risk and operating as intended while achieving and maintaining compliance with mandatory obligations?”



Example C: Tertiary Control

Internal Control for Independent Reasonable Assurance Audit

Risk Statement: The primary & secondary controls for monitoring, detection, review, and reconciliation of unauthorized configuration baseline changes is not being performed, is not operating as designed, and/or is ineffectively designed resulting in compromise of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).

Control Objective: Verify design effectiveness of primary & secondary controls and provide reasonable assurance execution conforms with expected cycles, actions, and documentation.

Control Activity Attributes:

Frequency:	Semi-annually not to exceed 6 calendar months
Responsible Party:	Internal Auditor
Activity:	Randomly selects six dates within the previous 6 calendar months each of which are within a different month (25% sample), independently re-performs the primary control activity for the calendar week of each sampled date, subsequently requests the official 'Example A' result records for the samples dates and performs a comparison and documents observations that are inconsistent with expected results.
Source(s):	<ol style="list-style-type: none"> 1. Baseline Monitoring Tool 2. Change Control Ticketing System 3. CIP-010-2 R2.1 Evidence Repository
Action Taken	Identified variances are researched (with consideration of any variances explained in secondary control records), unexplained deficiencies are documented, recommended actions are provided to the Manager of Responsible Party 'Example A' for the development of a management action plan, approved action plans are included in the monthly report to senior management, and tracked to completion to assure internal controls are sufficient and being executed as defined.

Control Activity Statement: On a semi-annual cycle not to exceed 6 calendar months, the Reliability Standards Internal Auditor (Internal Auditor), using RAT-STATS generates a 25% sample of dates contained within the previous 6 calendar months each of which are within a different month and independently re-performs the primary control activity for the calendar week of each date in the sample. Using authorized read-only access to the CIP-010-2 R2.1 Evidence Repository, the Internal Auditor retrieves copies of the 'Example A' result records for each date in the sample. The Internal Auditor performs a comparison between the re-performed control activities and the original records and documents observations that are inconsistent with expected results. Identified variances are researched (with consideration of any variances explained in secondary control records), unexplained deficiencies are documented, recommended actions are provided to the Manager of Responsible Party 'Example A' for the development of a management action plan. Approved action plans or acceptance of are included in Internal Auditor's the quarterly report to senior management and the Audit Committee, and tracked to completion to assure internal controls are sufficient and being executed as defined.



Risk Control Matrix:

A Risk Control Matrix (RCM) can be a helpful tool to inventory internal controls, and to document the relationships between them. This approach can also provide sustainability and serve as a road map for Registered Entities to mature from a manually maintained approach to the use of tools/ technology specifically designed to manage risk (sometimes referred to as eGRC).

Once the Control Statement is effectively designed and the control is implemented, and RCM can be used to help manage the oversight and assurance functions related to the controls. Often the information collected to create the Control Activity Statement is parsed out and each line item is given a unique Control ID.

Risk is normally in its own column, as well as Control Objective and Control Activity. Another field might logically be Standard and Requirement, Control Owner (or function), Frequency, etc. Other attributes are then associated like the control types previously discussed. In addition to this material data, source technology/application is usually listed. By inventorying controls in a linear format, that data can be sorted, filtered, and sliced-and-diced based on risk, resources, systems etc. Some examples of potential benefits are:

- Consider how common risks across the enterprise may become visible if inventoried in a centralized source.
- The CIP SMET has highlighted some instances where CIP-010-2 overlaps with elements of CIP-007-6. Consider how internal controls used to accomplish one requirement might support or achieve compliance with another requirement.
- Consider how an RCM could help manage workforce and priority. An RCM can be used to define a schedule for self-assessments and/or assurance audits based on risk, and it is flexible enough to add attributes to manage resources and timeframes associated to controls. Having this inventory can also help group common items and find synergies with work efforts so the same self-assessment and/or assurance audit can accomplish more than one objective at a time.
- A centralized source could also identify overlap across functions, and one group might gain efficiencies by leveraging controls that another group has more effectively designed. This holistic perspective can help reduce duplication of effort and aid program maturity.
- Consider the value that could be realized when replacing technology if an inventory of internal controls includes the source system. Registered Entities could use the RCM to get a holistic view of what controls that system provides, and which are key to not only maintaining compliance, but also to mitigate security and reliability risk. This extract could serve as a list of requirements for the new system to have confidence it can perform to expectations and meet regulatory obligations.

The next page is an illustration of an RCM, including the controls that were constructed using FRASA as well as a couple more. Similar to the [Rationale](#) for Requirement R2 and 3rd Party Tools within the Operational Controls Samples Section of this analysis, the following ideas for internal controls contain cycles and timeframes that are not prescribed within the Requirements. The frequency of these examples may exceed the minimums of the CIP Standard as a means to demonstrate how Registered Entities can layer safeguards to increase compliance margin and mitigate the risk of non-compliance through sound security practices.



Example Risk Control Matrix (RCM)											
Control ID	Standard, Req & Part	Risk Statement	Control Objective	Control Activities & Action Taken	Frequency	Responsible Party(ies)	Source	Control Type	Control Mechanism	Control Level	Related Controls
CCM-001	CIP-010-2 R2 Part 2.1	Unauthorized configuration baseline changes result in compromise of BES Cyber Systems and/or applicable Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES), concurrently causing non-compliance with mandatory regulatory obligations.	Detect and remediate any unapproved configuration baseline changes to reduce the risk of compromise of BES Cyber Systems and/or applicable Cyber Systems, while also maintaining compliance with mandatory regulatory obligations.	Monitors the alarm dashboard for detected baseline configuration changes. Compares detected changes to the Change Control Ticketing System and generates a high priority incident ticket for any discovered without an authorized change request. Monitors the dashboard until the alarm is cleared by the incident responder.	Each business day	On-call EMS Administrator	1. Baseline Monitoring Tool 2. Change Control Ticketing System	Key	Manual	Primary	CCM-002
CCM-002	CIP-010-2 R2 Part 2.1	Unauthorized configuration baseline changes result in compromise of BES Cyber Systems and/or applicable Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES), concurrently causing non-compliance with mandatory regulatory obligations.	Detect and remediate any unapproved configuration baseline changes to reduce the risk of compromise of BES Cyber Systems and/or applicable Cyber Systems, while also maintaining compliance with mandatory regulatory obligations.	Generates the "EMS BCA - Detected Baseline Configuration Changes" report and compares entries to the dashboard of approved EMS BCA changes within the Change Control Ticketing System and documents the results in an "Unauthorized Baseline Change Review Record" that is saved to the CIP-010-2 R2.1 Evidence Repository, even if results are null. Identified variances are researched, reconciled in accordance with change control processes and timelines, and reported by the end of the next business day to the compliance team and senior management for inclusion in corrective action program to mitigate the risk of recurrence and assure any mandatory regulatory reporting obligations are met.	Every 7 calendar days	On-call EMS Administrator	3. Baseline Monitoring Tool 4. Change Control Ticketing System	Non-Key	Manual	Primary	CCM-001
CCM-003	CIP-010-2 R2 Part 2.1	The primary control for monitoring, detection, review, and reconciliation of unauthorized configuration baseline changes is not being performed, or is not operating as designed, resulting in compromise of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).	Verify execution of primary control conforms with expected cycles, actions, documentation, and compliance timeframes.	Verifies a "Baseline Configuration Change Review Record" exists for each week in the previous calendar month, and that each record includes documented results of the expected comparison, any identified variances, and associated remediation actions, even if results are null. Identified missing or incomplete records, associated details, and risks of impending non-compliance with the 35 calendar day requirements are documented, added to the monthly conformance monitoring report, and distributed within 3 calendars days to the compliance team and senior management for risk assessment remediation within compliance timeframes.	The first business day of each calendar month	Reliability Standards Compliance Analyst	1. CIP-010-2 R2.1 Evidence Repository	Key	Manual	Secondary	CCM-002
CCM-004	CIP-010-2 R2 Part 2.1	The primary & secondary controls for monitoring, detection, review, and reconciliation of unauthorized configuration baseline changes is not being performed, is not operating as designed, and/or is ineffectively designed resulting in compromise of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).	Verify design effectiveness of primary & secondary controls and provide reasonable assurance execution conforms with expected cycles, actions, documentation, and compliance timeframes.	Randomly selects six dates within the previous 6 calendar months each of which are within a different month (25% sample), independently re-performs the primary control activity for the calendar week of each sampled date, subsequently requests the official 'Example A' result records for the samples dates and performs a comparison and documents observations that are inconsistent with expected results. Identified variances are researched (with consideration of any variances explained in secondary control records), unexplained deficiencies are documented, recommended actions are provided to the Manager of Responsible Party 'Example A' for the development a management action plan. A pproved action plans are included in the monthly report to senior management, and tracked to completion to assure internal controls are sufficient and being executed as defined.	Semi-annually not to exceed 6 calendar months	Internal Auditor	1. Baseline Monitoring Tool 2. Change Control Ticketing System 3. CIP-010-2 R2.1 Evidence Repository	Key	Manual	Secondary Tertiary	CCM-002 CCM-003
CCM-005	CIP-010-2 R2 Part 2.1	The system that monitors for configuration baseline changes is misconfigured or unavailable causing in an inability to detect unauthorized changes and generate reports needed to perform the primary control, resulting in unrealized unauthorized changes that lead to compromise	Verify the system that monitors for baseline configuration changes is functional and can detect and report as needed to assure ability to perform execution of primary control.	Monitors the health and status the Baseline Monitoring Tool once per hour, detects up/down status of the server, application, and/or needed ports and services, and reports unavailability or degraded performance to the Security Information & Event Management (SIEM) System.	Once per hour	1. System Health Monitoring Tool 2. Security Information & Event	1. Baseline Monitoring Tool	Non-Key	Automated	Secondary	CCM-002



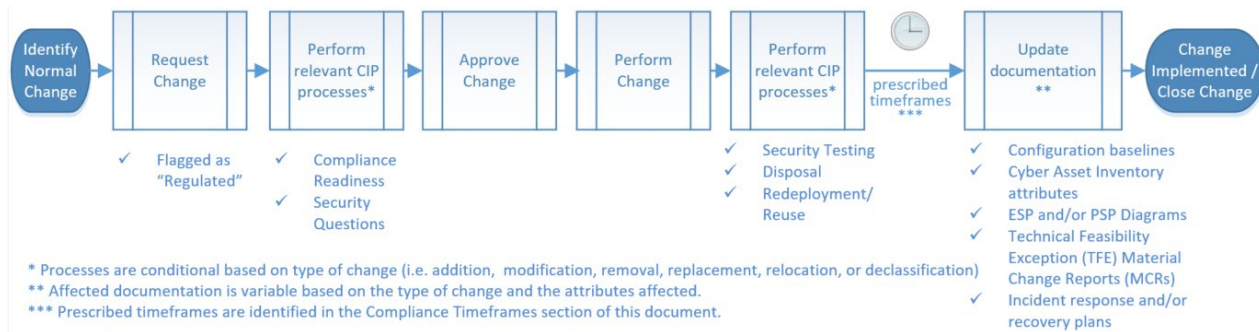
		of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).		Identified failures generate automated alerts that are distributed via email and text message to the system administrators of the Baseline Monitoring Tool, received alerts are investigated, and technical personnel troubleshoot and restore operability of the tool.		Management (SIEM) System					
CCM-006	CIP-010-2 R2 Part 2.1	The primary controls for monitoring, detection, review, and reconciliation of unauthorized configuration baseline changes is not being performed pursuant to the defined cycle causing a delay in the detection of unauthorized baseline changes resulting in compromise of BES Cyber Systems leading to misoperation or instability in the Bulk Electric System (BES).	Verify operational conformance to the defined cycle for performance of the secondary control to assure awareness of the need to execute activities.	Performs a check of the CIP-010-2 R2.1 Evidence Repository each Tuesday at 5:00 PM for the existence of an "Unauthorized Baseline Change Review Record" generated within the past two calendar days and having metadata with a status of "Complete". The absence of the expected record, creation date, and/or completion status causes the File System and Metadata Monitoring Tool to generate and automated Incident Ticket that is assigned to the EMS On Call Administrator. The Incident Ticket is prepopulated with the Control Activity Statement to provide instruction for the performance of the primary control and will autogenerate daily email reminders until complete.	Each Tuesday at 5:00 PM	1. File System and Metadata Monitoring Tool 2. Incident Ticketing System	1. CIP-010-2 R2.1 Evidence Repository	Non-Key	Automated	Tertiary	CCM-003



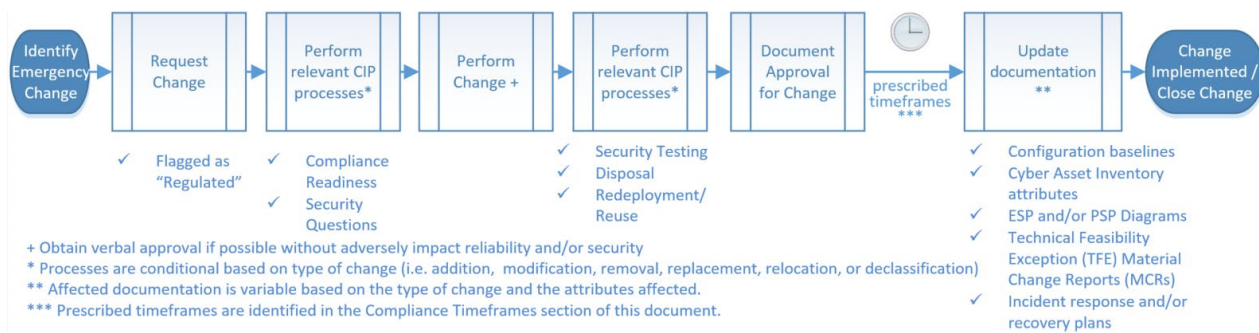
EXHIBIT A: REQUIREMENT R1, CONFIGURATION CHANGE MANAGEMENT (3RD PARTY TOOL OPTIONS)

Below are examples of possible process flow diagrams for various change categories:

Planned/Scheduled Change (ITIL Term = 'Normal Change')



Emergency/Unscheduled Change (ITIL Term = 'Emergency Change')



Pre-approved Routine Change (ITIL Term = 'Standard Change')

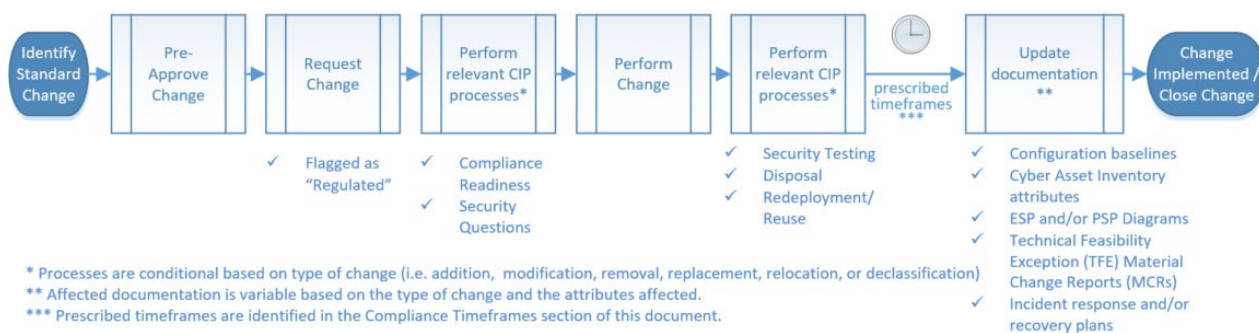


EXHIBIT B: PART 1.1 – ESTABLISHING BASELINES (MANUAL OPTIONS)

Below is an example of what the baseline attributes may look like. This illustrates a potential manual way of recording baselines. The 1st screenshotted is an excerpt from a spreadsheet formatted in landscape. This format would allow for filtering or grouping by baseline attributes.

Configuration Baselines for CIP-010-2 Requirement R1. Parts 1.1.1. - 1.1.5.										See other notes	FTP	FTP	SSH	Telnet	HTTP	61850	SSH (Service)	HTTPS	Modbus	Syslog	NETCONF	SSH					
Prepared by: Eustice C. Cured, Cybersecurity Analyst					Version: 01																						
Reviewed by: Justin Case, Lead Cybersecurity Analyst					Last updated: 6/15/2016						TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP	
Approved by: Boyd M. Goodman, Team Lead Cybersecurity					Effective Date: 7/1/2016																						
Approval Signature: <i>Boyd M. Goodman</i>					Approval Date: 6-28-2016						Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static	
Index	Cyber Asset ID	Cyber Asset Classification	Asset ID (Unique ID)	Cyber Asset Vendor	Cyber Asset Model	Operating System or Firmware Type	Operating System or Firmware Version	Security Patch Level / Service Pack		20	21	22	23	80	102	222	443	502	514	830							
1	FID-EAP-1	BCA	FID-EAP-1	Vendor 1	Model A	Firmware only	2.85	NA				X															
2	FID-ETH-1	PCA	FID-ETH-1	Vendor 2	Model B	Firmware only	v2.12	NA		X	X						X										
3	FID-HMI-1	BCA	FID-HMI-1	Vendor 3	Model C	Microsoft Windows 10 Pro	10 Pro	NA	X																		
4	FID-RTU-1	BCA	FID-RTU-1	Vendor 4	Model D	Firmware only	3.85.3	NA			X																
5	FID-IED-1	BCA	FID-IED-1	Vendor 5	Model E	Firmware only	7.81	NA						X				X									
6	FID-IED-2	BCA	FID-IED-2	Vendor 5	Model E	Firmware only	7.81	NA						X				X									

The landscape format was not conducive to displaying the long listing of port information and has been transposed for the purposes of illustrating its use to record logical network accessible ports.

Index	1	2	3	4	5	6
Cyber Asset ID	FID-EAP-1	FID-ETH-1	FID-HMI-1	FID-RTU-1	FID-IED-1	FID-IED-2
Cyber Asset Classification	BCA	PCA	BCA	BCA	BCA	BCA
Asset ID (Unique ID)	FID-EAP-1-SN:18279X	FID-ETH-1-SN:00QDEK	FID-HMI-1-SN:1F70AA2	FID-RTU-1-SN:202MR	FID-IED-1-SN:00354	FID-IED-2-SN:000355
Cyber Asset Vendor	Vendor 1	Vendor 2	Vendor 2	Vendor 3	Vendor 5	Vendor 5
Cyber Asset Model	Model A	Model B	Model C	Model D	Model E	Model E
Operating System or Firmware Type	Firmware only	Firmware only	Microsoft Windows	Firmware only	Firmware only	Firmware only
Operating System or Firmware Version	2.85	v2.12	10 Pro	3.85.3	7.81	7.81
Security Patch Level/Service Pack	NA	NA	NA	NA	NA	NA
See other notes			X			
Protocol Name	Protocol	Port No.				
FTP	TCP Static	20				
FTP	TCP Static	21				
SSH	TCP Static	22	X			
Telnet	TCP Static	23			X	
HTTP	TCP Static	80				
61850	TCP Static	102			X	X
SSH (Service)	TCP Static	222				
HTTPS	TCP Static	443	X			
Modbus	TCP Static	502			X	X
Syslog	TCP Static	514				
NETCONF	TCP Static	830				
SSH	TCP Static	922				
t2pnum	TCP Static	1024				
	TCP Static	1025				
IEC104	TCP Static	2404				
Eng Diagnostics	TCP Static	17185				
EGD Data port	TCP Static	18246				
DNP	TCP Static	20000			X	
DNP	TCP Static	20001				
SFTP	TCP Static	2222				
SQL database	TCP Static	5432				
TFTP	UDP Static	69				
SNTP	UDP Static	123				
SNMP	UDP Static	161				
SNMP	UDP Static	162		X		
Syslog	UDP Static	514	X		X	X
Radius	UDP Static	1812	X		X	X
Radius Accounting	UDP Static	1813	X			
PMU	TCP Static	4712				
PMU	UDP Static	4713				
PMU	UDP Static	4714				
DNP	UDP Static	20000				
DNP	UDP Static	20001		X		
	ICMP			X	X	X



This table is an example of how the port justification could be manually captured for groupings/categories of Cyber Asset.

Cyber Asset Grouping / Category & Corresponding Port Justification							
Protocol Name	Protocol Type	Port No.	Vendor 1 Model A	Vendor 2 Model B	Vendor 3 Model C	Vendor 4 Model D	Vendor 5 Model E
FTP	TCP	20					
FTP	TCP	21		Used for transferring files and upgrading firmware			
SSH	TCP	22	Provides a encrypted user interfaces for maintenance	Provides a encrypted user interfaces for maintenance			
Telnet	TCP	23					
HTTP	TCP	80					Cannot be disabled
61850	TCP	102					
SSH (Service)		222					
HTTPS	TCP	443		Provides a encrypted user interfaces for maintenance		Provides a encrypted user interfaces for maintenance	
Modbus	TCP	502					Required for Vendor software and cannot be disabled
Syslog	TCP	514					
NETCONF		830					
SSH	TCP	922					
t2pnum	TCP	1024					
Telnet	TCP	1025					
IEC104	TCP	2404					
Eng Diagnostics	TCP	17185					
EGD Data port	TCP	18246					
DNP	TCP	20000					
DNP	TCP	20001					
SFTP		2222					
SQL database	TCP	5432					
TFTP	UDP	69					
SNTP	UDP	123					
SNMP		161					
SNMP		162					
Syslog	UDP	514	Used to send syslogs to SIEM	Used to send syslogs to SIEM	Used to send syslogs to SIEM	Used to send syslogs to SIEM	Used to send syslogs to SIEM
Radius Accounting		1812					
PMU	TCP	4712					
PMU	UDP	4713					
PMU	UDP	4714					
DNP	UDP	20000					
DNP	UDP	20001					
ICMP	ICMP		Disabled	Disabled at network firewall; allowed inside networks	Disabled at network firewall; allowed inside networks	Disabled at network firewall; allowed inside networks	Disabled at network firewall; allowed inside networks

This table is an example of how the software inventory of Cyber Assets might be manually maintained yet correlated to a baseline spreadsheet/table via reference:

Index	1	2	3	4	5	6
Cyber Asset ID	FID-EAP-1	FID-ETH-1	FID-HMI-1	FID-RTU-1	FID-IED-1	FID-IED-2
Cyber Asset Classification	BCA	PCA	BCA	BCA	BCA	BCA
Asset ID (Unique ID)	FID-EAP-1-SN:18279X	FID-ETH-1-SN:00QDEK	FID-HMI-1-SN:1F70AA2	FID-RTU-1-SN:202MR	FID-IED-1-SN:00354	FID-IED-2-SN:000355
Cyber Asset Vendor	Vendor 1	Vendor 2	Vendor 2	Vendor 3	Vendor 5	Vendor 5
Cyber Asset Model	Model A	Model B	Model C	Model D	Model E	Model E
Operating System or Firmware Type	Firmware only	Firmware only	Microsoft Windows	Firmware only	Firmware only	Firmware only
Operating System or Firmware Version	2.85	v2.12	10 Pro	3.85.3	7.81	7.81
Security Patch Level/Service Pack	NA	NA	NA	NA	NA	NA
Other notes	NA	NA	Referenced files for Software Inventory exports are stored in secured evidence locker @ https://entityx/cip-010-R1.1/	NA	NA	NA
Installed Comerically Available Software	NA	NA	Windows Registry Export MMDDYY.txt	NA	NA	NA
Installed Open-source Software	NA	NA	Windows Registry Export MMDDYY.txt	NA	NA	NA
Installed Open-source Software	NA	NA	Windows Registry Export MMDDYY.txt	NA	NA	NA



EXHIBIT C: PART 1.1.1. – OPERATING SYSTEM OR FIRMWARE VERSIONS (3RD PARTY TOOL OPTIONS)

This is a sample report from a Microsoft Windows 7 based Cyber Asset. Note the BIOS version and the Operating System are both captured in the baseline report

Element Contents

Date:	6/28/18 10:51 AM
Maximum lines displayed (0 = all lines):	0
Only include versions with content:	Yes
Group by:	Nodes
Audit events:	(Any)
Display criteria at end:	No
Use strict package match:	No
Node Names:	[REDACTED]
Rules:	CIP-010-2, R1 BIOS Version, CIP-010-2, R1.1.1 Operating System
Current versions only:	Yes
Change types:	Added, Modified, Removed, Baseline
Nodes sort:	Name, ascending
Rules sort:	Name, ascending

[REDACTED] (Windows Server)

CIP-010-2, R1 BIOS Version (Command Output Capture Rule)

CIP-010-2, R1 BIOS Version

Version :	1/11/18 12:20 PM
Type :	Baselined
Content	<pre>"SystemBiosDate"="12/21/17" "SystemBiosVersion"=hex(7):44,00,45,00,4c,00,4c,00,20,00,20,00,20,00,2d,00,20,\ "VideoBiosDate"="06/24/15" "VideoBiosVersion"=hex(7):56,00,65,00,72,00,73,00,69,00,6f,00,6e,00,20,00,38,\ "BiosMajorRelease"=dword:00000041 "BiosMinorRelease"=dword:00000018 "BIOSReleaseDate"="12/21/2017" "BIOSVendor"="Dell Inc." "BIOSVersion"="A24"</pre>

CIP-010-2, R1.1.1 Operating System (Command Output Capture Rule)

CIP-010-2, R1.1.1 Operating System

Version :	6/4/17 11:45 AM
Type :	Baselined
Content	6.1.7601

Total Elements: 2



EXHIBIT D: PART 1.1.1. – OPERATING SYSTEM OR FIRMWARE VERSIONS (MANUAL OPTIONS)

Below is a sample script that can be run on a Microsoft Windows platform to gather the operating system version as well as a lot of system properties and writes the output to a text file for evidence. The output file contains the name of the cyber asset, date, and time the script was executed.

```
' Export System Information.vbs
'
'=====
' Set up the script variables.
'=====
Set oNetwork = CreateObject("Wscript.Network")
strComputer = oNetwork.ComputerName
Set oShell = Wscript.CreateObject("Wscript.Shell")
strDate = Replace(Replace(FormatDateTime(Now(),2),"/","-")," ","_")
strTime = Replace(FormatDateTime(Now(),3),":","-")
strFile = oShell.CurrentDirectory & "\" & strComputer & "_System-Information_" & strDate & "_" & strTime & ".txt"
strBatch = oShell.CurrentDirectory & "\" & strDate & "_" & strTime & ".bat"
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFile = oFSO.CreateTextFile(strFile)
Set oBatch = oFSO.CreateTextFile(strBatch)
strProgram = Chr(34) & "C:\Program Files\Common Files\Microsoft Shared\MSInfo\msinfo32.exe" & Chr(34)
'=====
' Close the files and run the batch file.
'=====
oBatch.WriteLine strProgram & " /report " & Chr(34) & strFile & Chr(34)
oFile.Close
oBatch.Close
oShell.Run Chr(34) & strBatch & Chr(34), 3, True
oFSO.DeleteFile strBatch
'=====
' Clean up.
'=====
Set oBatch = Nothing
Set oFile = Nothing
Set oFSO = Nothing
Set oShell = Nothing
Set oNetwork = Nothing
Wscript.Echo "Script complete, please check for the following output file:" & vbCr & vbCr & strFile
```



EXHIBIT E: PART 1.1.2. & 1.1.3 – COMMERCIAL, OPEN-SOURCE, OR CUSTOM SOFTWARE (3RD PARTY TOOL OPTIONS)

Below is an example of what the baseline attributes may look like. This is the first page of a report from a 3rd part tool. Depending on the number of software installations the report may vary in length

Element Contents

Date:	6/28/18 11:13 AM
Maximum lines displayed (0 = all lines):	0
Only include versions with content:	Yes
Group by:	Nodes
Audit events:	(Any)
Display criteria at end:	No
Use strict package match:	No
Node Names:	██████████
Rules:	CIP-010-2, R1.1.2 Commercial Software (Java), CIP-010-2, R1.1.2 Commercial Software (Meinberg), CIP-010-2, R1.1.2 Commercial Software (Nmap), CIP-010-2, R1.1.2 Installed Programs
Current versions only:	Yes
Change types:	Added, Modified, Removed, Baseline
Nodes sort:	Name, ascending
Rules sort:	Name, ascending

██████████ (Windows Server)

CIP-010-2, R1.1.2 Commercial Software (Meinberg) (Command Output Capture Rule)

CIP-010-2, R1.1.2 Commercial Software (Meinberg)

Version :	4/27/18 4:59 PM
Type :	Baselined
Content	
DisplayName DisplayVersion ----- Network Time Protocol 4.2.8p11	

CIP-010-2, R1.1.2 Installed Programs (Command Output Capture Rule)

CIP-010-2, R1.1.2 Installed Programs

Version :	6/28/18 11:13 AM
Type :	Baselined
Content	
[BEGIN] Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall] [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\4AE6C528D40463ED98CD9356341B7EF2CFFF20DE] "UninstallString"="C:\PROGRAMS\1\B60D1297D6D5E54C\DPInst.exe /u C:\Windows\system32\DRVSTORE\legminflt_7F9C0B092E88C3A476D9F5A41BF49C3EC2200025\legmin	



Sample CurrPorts.reg.txt Script

Below is an example of a script to register the custom software installation attributes on a Windows machine:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CurrPorts.exe]
```

```
"DisplayName"="CurrPorts.exe"
```

```
"DisplayVersion"="2.20"
```

```
"Publisher"="NirSoft (Nir Sofer)"
```

```
"InstallDate"="20150825"
```

```
"HelpLink"="http://www.nirsoft.net/utills/cports.html"
```

```
"InstallLocation"="C:\\NERC\\CIP\\007-3\\R2\\CurrPorts"
```

```
"InstallSource"="N:\\Software\\CurrPorts"
```

```
"URLInfoAbout"="http://www.nirsoft.net/utills/cports.html"
```

```
"DisplayIcon"="C:\\NERC\\CIP\\007-3\\R2\\CurrPorts\\cports.exe"
```

```
"Comments"="Monitoring Opened TCP/IP Network Ports / Connections"
```

```
"Contact"="your_support_contact@your_company.com"
```

```
"WindowsInstaller"=dword:00000000
```

```
"UninstallString"="C:\\NERC\\CIP\\007-3\\R2\\CurrPorts\\cports.exe"
```

```
"EstimatedSize"=dword:00000048
```



EXHIBIT F: PART 1.1.2. & 1.1.3 – COMMERCIAL, OPEN-SOURCE, OR CUSTOM SOFTWARE (MANUAL OPTIONS)

Below is an example of a batch script for manually querying a Windows machine for installed software:

```
'
' Export Installed Programs.vbs
'=====
' Set up the script variables.
'=====
Set oNetwork = CreateObject("Wscript.Network")
strComputer = oNetwork.ComputerName
Set oShell = Wscript.CreateObject("Wscript.Shell")
strDate = Replace(Replace(FormatDateTime(Now(),2),"/","-")," ","_")
strTime = Replace(FormatDateTime(Now(),3),":","-")
strFile = oShell.CurrentDirectory & "\ " & strComputer & "_Installed-Programs_" & strDate & "_" & strTime & ".txt"
strBatch = oShell.CurrentDirectory & "\ " & strDate & "_" & strTime & ".bat"
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFile = oFSO.CreateTextFile(strFile)
Set oBatch = oFSO.CreateTextFile(strBatch)
strProgram = "regedit.exe"
'=====
' Close the files and run the batch file.
'=====
oBatch.WriteLine strProgram & " /E " & Chr(34) & strFile & Chr(34) & "
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall"
oFile.Close
oBatch.Close
oShell.Run Chr(34) & strBatch & Chr(34), 3, True
oFSO.DeleteFile strBatch
'=====
' Export the Microsoft KB information.
'=====
MsgBox "Please wait until the list of KB patches is complete!" & vbCr & vbCr & "Click 'OK' to export KB information...",48,"WAIT!"
forwOnly = &h20
forAppend = 8

Set oFile = oFSO.OpenTextFile(strFile,forAppend,True,-1)

Set objWMIService = GetObject("winmgmts:\\.\\root\CIMV2")

Set cols = objWMIService.ExecQuery("SELECT * FROM Win32_QuickFixEngineering","WQL",retImm + forwOnly)
```



For Each obj In cols

```
oFile.WriteLine "[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall" & obj.HotFixID & "]"
```

```
oFile.WriteLine Chr(34) & "DisplayName" & Chr(34) & "=" & Chr(34) & obj.HotFixID & Chr(34)
```

```
oFile.WriteLine Chr(34) & "InstallDate" & Chr(34) & "=" & Chr(34) & obj.InstalledOn & Chr(34)
```

```
oFile.WriteLine Chr(34) & "DisplayVersion" & Chr(34) & "=" & Chr(34) & obj.ServicePackInEffect & Chr(34)
```

```
oFile.WriteLine Chr(34) & "URLInfoAbout" & Chr(34) & "=" & Chr(34) & obj.Caption & Chr(34)
```

```
oFile.WriteLine
```

Next

```
oFile.Close
```

```
'=====
```

```
' Clean up.
```

```
'=====
```

```
Set oBatch = Nothing
```

```
Set oFile = Nothing
```

```
Set oFSO = Nothing
```

```
Set oShell = Nothing
```

```
Set oNetwork = Nothing
```

```
Wscript.Echo "Script complete, please check for the following output file:" & vbCr & vbCr & strFile
```



EXHIBIT G: PART 1.1.4. – LOGICAL NETWORK ACCESSIBLE PORTS (3RD PARTY TOOL OPTIONS)

Element Contents

Date:	6/28/18 11:15 AM
Maximum lines displayed (0 = all lines):	0
Only include versions with content:	Yes
Group by:	Nodes
Audit events:	(Any)
Display criteria at end:	No
Use strict package match:	No
Rules:	Nmap Port Scans
Element names:	Contains [REDACTED]
Current versions only:	Yes
Change types:	Added, Modified, Removed, Baseline
Nodes sort:	Name, ascending
Rules sort:	Name, ascending

[REDACTED] (Windows Server)

CIP-010-2, R1.1.4 Logical Nmap Ports [REDACTED] (Command Output Capture Rule)

CIP-010-2, R1.1.4 Logical Nmap Ports [REDACTED]

Version : 6/27/18 10:22 AM
Type : Baselined
Content

```

*** Beginning Nmap Scan...
nmap -sS -sU -Pn -p 1-65535 --max-scan-delay 50ms -max-retries 2 -v
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-23 13:00 Central Daylight Time
e
Initiating ARP Ping Scan at 13:00
Scanning [REDACTED] [1 port]
Completed ARP Ping Scan at 13:00, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:00
Completed Parallel DNS resolution of 1 host. at 13:00, 0.01s elapsed
Initiating SYN Stealth Scan at 13:00
Scanning [REDACTED] [65535 ports]
Completed SYN Stealth Scan at 13:13, 819.18s elapsed (65535 total ports)
Initiating UDP Scan at 13:13
Scanning [REDACTED] [65535 ports]
Completed UDP Scan at 13:15, 110.39s elapsed (65535 total ports)
Nmap scan report for [REDACTED]
Host is up (0.00s latency).
rDNS record for [REDACTED]
Not shown: 65535 open|filtered ports, 65532 filtered ports
PORT STATE SERVICE
6666/tcp open irc
9898/tcp open monkeycom
12345/tcp open netbus
MAC Address: [REDACTED]
Read data files from: C:\Progra~2\Nmap
Nmap done: 1 IP address (1 host up) scanned in 930.09 seconds
Raw packets sent: 262270 (9.449MB) | Rcvd: 2556 (169.692KB)
    
```

Total Elements: 1



EXHIBIT H: PART 1.1.4. – LOGICAL NETWORK ACCESSIBLE PORTS (MANUAL OPTIONS)

Below is an example of a batch script for manually exporting port with netstat:

Export Netstat Ports.vbs

```
'
'=====
' Set up the script variables.
'=====
Set oNetwork = CreateObject("Wscript.Network")
strComputer = oNetwork.ComputerName
Set oShell = Wscript.CreateObject("Wscript.Shell")
strDate = Replace(Replace(FormatDateTime(Now(),2),"/","-")," ","_")
strTime = Replace(FormatDateTime(Now(),3),":","-")
strFile = oShell.CurrentDirectory & "\" & strComputer & "_Netstat-Ports_" & strDate & "_" & strTime & ".txt"
strBatch = oShell.CurrentDirectory & "\" & strDate & "_" & strTime & ".bat"
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oFile = oFSO.CreateTextFile(strFile)
Set oBatch = oFSO.CreateTextFile(strBatch)
strProgram = "netstat.exe"
'=====
' Close the files and run the batch file.
'=====
oBatch.WriteLine strProgram & " -abon > " & Chr(34) & strFile & Chr(34)
oFile.Close
oBatch.Close
oShell.Run Chr(34) & strBatch & Chr(34), 3, True
oFSO.DeleteFile strBatch
'=====
' Clean up.
'=====
Set oBatch = Nothing
Set oFile = Nothing
Set oFSO = Nothing
Set oShell = Nothing
Set oNetwork = Nothing

Wscript.Echo "Script complete, please check for the following output file:" & vbCr & vbCr & strFile
```



Below is an example of a batch script for manually extracting TCP-UDP ports using nmap:

Export Nmap Ports Full TCP-UDP.vbs

```
'
' Function: The purpose of this script is to run an Nmap scan and direct output to specific filenames.
'
' Revision History:
'
'=====
' Set up the script variables.
'=====

Set oNetwork = CreateObject("Wscript.Network")

strIpAddr = InputBox("Please enter the IP address to scan:","Enter IP Address","127.0.0.1")

strDevice = oNetwork.ComputerName

strDevice = InputBox("Please enter the device name for output filenames:","Enter Device Name",strDevice)

strDevice = UCase(strDevice)

Set oShell = Wscript.CreateObject("Wscript.Shell")

strDate = Replace(Replace(FormatDateTime(Now(),2),"/","-")," ","_")

strTime = Replace(FormatDateTime(Now(),3),":","-")

strFile = oShell.CurrentDirectory & "\" & strDevice & "\Nmap Ports\" & Year(strDate) & "\" & strDevice & "_Nmap-Ports_" & strDate & "_" & strTime & ".nmap"

strBatch = oShell.CurrentDirectory & "\" & strDevice & "_Nmap-Ports_" & strDate & "_" & strTime & ".bat"

Set oFSO = CreateObject("Scripting.FileSystemObject")

Set oBatch = oFSO.CreateTextFile(strBatch)

strProgram = Chr(34) & "C:\Program Files (x86)\Nmap\nmap.exe" & Chr(34) & " -sS -sU -p 1-65535 -v " & strIpAddr

'=====
' Close the files and run the batch file.
'=====

oBatch.WriteLine "mkdir " & Chr(34) & strDevice & Chr(34)
```



```
oBatch.WriteLine "mkdir " & Chr(34) & strDevice & "\Nmap Ports" & Chr(34)

oBatch.WriteLine "mkdir " & Chr(34) & strDevice & "\Nmap Ports\" & Year(strDate) & Chr(34)

oBatch.WriteLine strProgram & " -oN " & Chr(34) & strFile & Chr(34)

oBatch.Close

oShell.Run Chr(34) & strBatch & Chr(34), 3, True

oFSO.DeleteFile strBatch

'=====

' Clean up.

'=====

Set oBatch = Nothing

Set oFSO = Nothing

Set oShell = Nothing

Set oNetwork = Nothing

Wscript.Echo "Script complete, please check for the following output file:" & vbCr & vbCr & strFile
```



EXHIBIT I: PART 1.1.5. – APPLIED SECURITY PATCHES (3RD PARTY TOOL OPTIONS)

Below is an example of what the applied security patch attributes may look like. This is the first page of a report from a 3rd party tool. Depending on the number of applied security patches, the report length may vary.

Element Contents

Date:	6/28/18 11:17 AM
Maximum lines displayed (0 = all lines):	0
Only include versions with content:	Yes
Group by:	Nodes
Audit events:	(Any)
Display criteria at end:	No
Use strict package match:	No
Node Names:	[REDACTED]
Rules:	CIP-010-2, R1.1.5 Security Patches (WinUpdatesList)
Current versions only:	Yes
Change types:	Added, Modified, Removed, Baseline
Nodes sort:	Name, ascending
Rules sort:	Name, ascending

[REDACTED] (Windows Server)

CIP-010-2, R1.1.5 Security Patches (WinUpdatesList) (Command Output Capture Rule)

CIP-010-2, R1.1.5 Security Patches (WinUpdatesList)

```

Version :                               6/27/18 12:54 PM
Type :                                   Baselined
Content
Remote Share [REDACTED]
Remote User: [REDACTED]
Local Directory: C:\Windows\Temp
Connecting remote share...
The command completed successfully.
Retrieving remote program...
[REDACTED]
1 file(s) copied.
Building local configuration file...
C:\Windows\Temp\wul.cfg
Executing local program...
C:\Windows\Temp\wul.exe
Reading local output...
C:\Windows\Temp\wul.txt
[BEGIN]
=====
Name : KB2565063
Description : Hotfix for Microsoft Visual C++ 2010 x84 Redistributable (K
B2565063)
Installed By : Administrator
Installation Date : 12/11/2015
Display Version :
Update Type :
Web Link : http://support.microsoft.com/kb/2565063
Last Modified Time: 6/3/2017 1:18:47 PM
=====
Name : KB2565063
Description : Hotfix for Microsoft Visual C++ 2010 x86 Redistributable (K
B2565063)
Installed By : Administrator
Installation Date : 12/11/2015
Display Version :
Update Type :
Web Link : http://support.microsoft.com/kb/2565063
Last Modified Time: 6/3/2017 1:18:47 PM
=====
                    
```

CLARITY

ASSURANCE

RESULTS

146

EXHIBIT J: PART 1.1.5. – APPLIED SECURITY PATCHES (MANUAL OPTIONS)

Caption	CSName	Description	FixComments	HotFixID	InstallDate	InstalledBy	InstalledOn	Name	ServicePackInEffect	Status
http://support.microsoft.com/kb/2889189	S000	Update		KB2889189_Microsoft-Windows-CameraCodec-Package		NT AUTHORITY\SYSTEM	6/21/2015			
http://support.microsoft.com/?kbid=2919355	S000	Update		KB2919355		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2919442	S000	Update		KB2919442		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2934520	S000	Update		KB2934520		NT AUTHORITY\SYSTEM	6/19/2015			
http://support.microsoft.com/?kbid=2937220	S000	Update		KB2937220		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2938772	S000	Update		KB2938772		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2939471	S000	Update		KB2939471		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2949621	S000	Hotfix		KB2949621		S000\Administrator	3/18/2014			
http://support.microsoft.com/?kbid=2954879	S000	Update		KB2954879		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2967917	S000	Update		KB2967917		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2973351	S000	Security Update		KB2973351		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2975061	S000	Update		KB2975061		NT AUTHORITY\SYSTEM	6/19/2015			
http://support.microsoft.com/?kbid=2976978	S000	Update		KB2976978		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2977765	S000	Security Update		KB2977765		NT AUTHORITY\SYSTEM	6/19/2015			
http://support.microsoft.com/?kbid=2978126	S000	Security Update		KB2978126		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2989930	S000	Update		KB2989930		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=2990967	S000	Update		KB2990967		NT AUTHORITY\SYSTEM	6/19/2015			
http://support.microsoft.com/?kbid=2994290	S000	Update		KB2994290		NT AUTHORITY\SYSTEM	6/19/2015			
http://support.microsoft.com/?kbid=3000850	S000	Update		KB3000850		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3003057	S000	Security Update		KB3003057		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3003667	S000	Update		KB3003667		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3004361	S000	Security Update		KB3004361		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3004365	S000	Security Update		KB3004365		NT AUTHORITY\SYSTEM	9/2/2015			
http://support.microsoft.com/?kbid=3004394	S000	Update		KB3004394		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3006137	S000	Update		KB3006137		NT AUTHORITY\SYSTEM	6/22/2015			
http://support.microsoft.com/?kbid=3008242	S000	Update		KB3008242		NT AUTHORITY\SYSTEM	6/22/2015			

EXHIBIT K: PART 1.2. – AUTHORIZING & DOCUMENTING BASELINE DEVIATIONS (3RD PARTY TOOL OPTIONS)

In this example, a 3rd Party Tool is used to route the approval request for a baseline change via workflow to the respective owner of the Cyber Asset. The system stamps the record with the approval. Some data has been intentionally obfuscated within this screen capture.

Change Workflow State: Initiation Review/Approval Execution PIR Closed

Type: Normal
Status: Closed
Completion Code: Successful
Priority: 3 - Medium
Requestor: [Redacted]

Owned By Team/Change Owner
EMS Admins
System Operations Administrator

Classify
Type of Change: NERC Regulated PIR
 Manager Approval Required
Change Title: June 2018 Scheduled Updates for Microsoft
Description: Install updates in development and production environments.

Change Type: Software Modify Existing | Category: Release Management | Subcategory: Security Patch | Priority: 3 - Medium



Schedule
Planned Start: 7/12/2018 12:00 AM | Actual Production Start: 7/28/2018 2:27 PM
Planned End: 9/12/2018 12:00 AM | Actual Production End: 8/24/2018 12:10 PM

Change Status	Change ID	Title	Approver	Approval Status	Approver Comment	Deadline
Approved			[Redacted]	Approved	Approved for production roll-out.	



EXHIBIT L: PART 1.2. – AUTHORIZING & DOCUMENTING BASELINE DEVIATIONS (MANUAL OPTIONS)

Sample Manual Approval Record

 Registered Entity X		NERC CIP CYBER ASSET BASELINE CONFIGURATION CHANGE CONTROL RECORD	
NERC CIP CYBER ASSET BASELINE CONFIGURAITON CHANGE RECORD			
This change control form, when completed, constitutes the official record of evidence in alignment with the below indicated version of the NERC CIP Reliability Standards concurrent with the dated signature on this form.			
Requirement(s):		CIP-010-2 R1 Part 1.2	
Cyber Asset Name(s):		adserver-123-parklawn, authserver-acb-lu7xusave	
Subject Matter Expert Name:		Justin Case	Subject Matter Expert Title: Lead Cybersecurity Analyst
Change Request			
Change Type: <i>(Check All That Apply)</i>		<input type="checkbox"/> Install New <input checked="" type="checkbox"/> Modify <input type="checkbox"/> Remove <input type="checkbox"/> Relocate <input type="checkbox"/> De-Classify	
Change Object: <i>(Check All That Apply)</i>		<input checked="" type="checkbox"/> Operating System/Firmware <input type="checkbox"/> Commerical/Open-source Software <input type="checkbox"/> Custom Software <input checked="" type="checkbox"/> Network Accessible Logical Ports and Services <input checked="" type="checkbox"/> Security Patches	
Change Description:		Upgrade from Windows Server 2003 to Windows Server 2008, update ports and services to align with last approved Windows Server 2008 baseline, install all applicable security patches.	
Change Request Date:		6/15/2016	Proposed Implementation Date or Timeframe: 7/1/2016
Change Circumstance: <i>(Check One)</i>		<input checked="" type="checkbox"/> Non-Emergency <input type="checkbox"/> Emergency	
Required Activities : <i>(Check All That Apply)</i>		<input type="checkbox"/> Compliance Readiness for New Hardware <input checked="" type="checkbox"/> Security Posture Test for Significant Change(s) <input type="checkbox"/> Disposal or Redeployment for Hardware Removals	
Change Approval			
The signature below indicates the formal review and approval of the proposed change, as well as associated compliance obligations and timeline, as required by the NERC CIP Reliability Standards.			
Approver Name:		Boyd M. Goodman	Approver Title: Team Lead Cybersecurity
Approver Signature:			Approval Date: 6.28.2016

Manual Form Design Considerations

- As a design consideration, it may be helpful to indicate if fields are required, optional, or conditional (triggered) to give the approver clarity on if the form is complete.
- Consider incorporating instructions into the paper form to repeatability communicate expectations when filling it out, and to help achieve consistency with records. Simple details like these may help to reduce



the risk of human performance errors that often carry a higher likelihood of occurrence with manual solutions.

- Consider leveraging techniques that allow the user to circle a predefined value or check a box, especially where normalized data is sought, and user discretion/interpretation is not required. This can add efficiency, consistency, prevent invalid/illegible conditions. Simple design considerations like these may help streamline the process while alleviating administrative burden for end users, reviewers and approvers. As an example, it is important to know what type of change is occurring; below demonstrates alternative way to capture that information:

Identify the Change Type (required)	
Option A	<hr/> (enter the type of change)
Option B	Move / Add / Change / Replace / Remove (circle one)
Option C	<input type="checkbox"/> Move <input type="checkbox"/> Add <input type="checkbox"/> Change <input type="checkbox"/> Replace <input type="checkbox"/> Remove (check one)
Option D	<input type="checkbox"/> Move <input type="checkbox"/> Add <input type="checkbox"/> Change <input type="checkbox"/> Replace <input type="checkbox"/> Remove <input type="checkbox"/> Other <hr/> (Check one. If Other, please explain)

- Consider providing a set of quality checks for the approver to run through before signing. As an example, a checklist is one approach that could include things like:
 - Are all the required fields completed?
 - Is the form legible?
 - Is the person performing the change the correct person to work on the Cyber Assets listed?
 - Does the business need justify the urgency or timing of the request?
 - Is the change implementation date in the future?



EXHIBIT N: PART 1.4. – ASSESSING AND TESTING CYBER SECURITY CONTROLS (3RD PARTY TOOL OPTIONS)

Sample of a 3rd Party Tool with programmatic logic based on change type and Cyber Asset capability profile being used to perform pre-change security impact assessment for regulated changes. Any logic programmed into a system is dependent on the Registered Entity’s methodology and criteria used. This is an example only and not intended to be an all-inclusive list of questions that a system may prompt for.

The screenshot shows a software interface for a change management system. At the top, it indicates the 'Change Type' is 'Standard' and the 'Workflow State' is 'Closed'. The change title is 'Server Patching Scheduled - Prod'. Below this, there is a navigation bar with various icons and labels like 'PIR', 'Planning', 'Configuration Items', 'Journals', 'History', 'Current Reviewers', 'Tasks', 'Master Tasks', 'Answered Questions', 'Related Change', and 'Incidents'. The main area displays a table of security questions related to the change.

Question #	Security Question Text	Created Date Time	CI Name	CI Alias	Answer
2	Could the change affect allowable inbound/outbound access from outside the ESP?	8/16/2016 10:55 AM			No
4	Could the change affect installed malicious communication detection tools?	8/16/2016 10:55 AM			No
5	Could the change affect Interactive Remote Access (IRA) controls?	8/16/2016 10:55 AM			No
6	Could the change affect intermediate System controls required for interactive Remote Access (IRA)?	8/16/2016 10:55 AM			No
8	Could the change affect a PSP diagram(s)?	8/16/2016 10:55 AM			No
9	Could the change affect physical access monitoring controls?	8/16/2016 10:55 AM			No
10	Could the change affect PSP logging controls?	8/16/2016 10:55 AM			No
11	Could the change affect physical access alarming/alerting controls?	8/16/2016 10:55 AM			No
12	Could the change affect open logical ports and services?	8/16/2016 10:55 AM			No
14	Could the change revert implemented mitigations for applicable security patches not installed?	8/16/2016 10:55 AM			Y88
15	Could the change affect installed malicious code prevention tools?	8/16/2016 10:55 AM			Yes
16	Could the change affect the Cyber Asset's local security event logging?	8/16/2016 10:55 AM			Yes
17	Could the change affect log settings for sending and remote receiving so as to potentially affect s...	8/16/2016 10:55 AM			Yes
18	Could the change affect the Cyber Asset's local log retention?	8/16/2016 10:55 AM			No
22	Could the change affect "account lockout" controls?	8/16/2016 10:55 AM			No
23	Could the change affect how a user locally authenticates to the Cyber Asset?	8/16/2016 10:55 AM			No
24	Could the change affect account configuration (shared, generic, or default accounts)?	8/16/2016 10:55 AM			



EXHIBIT O: PART 1.4. – ASSESSING AND TESTING CYBER SECURITY CONTROLS (MANUAL OPTIONS)

Sample of a manual approach to assessing and verifying cybersecurity controls. This is an example only, and not intended to be an all-inclusive list. The sample record was derived using the four tables provided in the Supporting Analysis section of CIP-010-2 Requirement R1 Part 1.4 of this SAG.

[Table 1 – CIP-005 Cybersecurity Controls](#)

[Table 2 – CIP-007 Cybersecurity Controls](#)

[Table 3 – CIP-005 Cybersecurity Controls Verification](#)

[Table 4 – CIP-007 Cybersecurity Controls Verification](#)


 Registered Entity X		NERC CIP CYBER ASSET BASELINE CONFIGURATION SECURITY IMPACT ASSESSMENT AND TESTING RECORD						
Related Change Record: 1028927492		Assessment Date: 6/15/2016 Change Date: 7/1/2016 Post-Change Verification Date: 7/2/2016						
Subject Matter Expert Name: Justin Case								
Subject Matter Expert Title: Lead Cybersecurity Analyst								
Cyber Asset(s) undergoing Baseline Configuration Change	Requirement & Part Evaluated Pre-Change	Associated Security Control(s) Assessed for Impact Pre-Change	Is Impacted (Yes/No)	Security Control(s) Verification Steps	Post-Change Verification Results (Pass, Fail) If Fail, specify Post-Actions & Final Verified Status	Post-Actions Taken to Secure (Used Lessons Learned)	Final Verified Status (Corrected, Rolled Back, Mitigated)	Captured Evidence
adserver-123-parklawn	CIP-005-5 R1	ESP	No		NA	NA	NA	NA
authserver-acb-lu7xusave	CIP-005-5 R1	ESP	No		Pass	NA	NA	NA
adserver-123-parklawn	CIP-007-6 R1	Open Network Accessible Ports	Yes	Run netstat, nmap, and tcpdump	Pass	NA	NA	netstat, nmap, and tcpdump outputs
authserver-acb-lu7xusave	CIP-007-6 R1	Open Network Accessible Ports	Yes	Run netstat, nmap, and tcpdump	Fail	Telnet was open after changes. Disabled manually.	Corrected	netstat, nmap, and tcpdump outputs including pre- and post-correction
adserver-123-parklawn	CIP-007-6 R2	Security Patch Level	Yes	Run batch script to verify patch install.	Pass	NA	NA	batch script output registry screenshot
authserver-acb-lu7xusave	CIP-007-6 R2	Security Patch Level	Yes	Run batch script to verify pathc install.	Pass	NA	NA	



EXHIBIT P: PART 1.5. – TESTING HIGH IMPACT BASELINE CHANGES (MANUAL OPTIONS)

Sample security testing questionnaire:

Security Test Question	Response YES/NO	Manual Evidence
Could ports and services be impacted by the change?		SME can run the netstat command and compare the output to the baseline to ensure ports and services were not affected.
Could physical ports be impacted by the change?		SME can test physical port by looking at physical port LED and within the device configuration to ensure they were not affected.
Could the operating system(s), including version, or firmware be impacted by the change?		A screenshot of the operating system and firmware can be compared with the baseline to ensure they were not affected.
Could the installed software be impacted by the change?		A screenshot of installed software showing the version can be compared to the baseline to ensure the control was not affected.
Could the security patch level be impacted by the change?		SME can generate an output of patch level and compare to the baseline to ensure patch level was not affected.
Could malicious code prevention controls be impacted by the change?		SME can test the malicious code prevention controls by making sure the service is still running to ensure they were not affected by the change.
Could security event alert controls be impacted by the change?		SME can test the security event alert control by manually generating alerts to ensure they were not affected by the change.
Could ESP controls be impacted by the change?		SME can test the ESP controls by doing a network scan and reviewing the logs to ensure they were not affected by the change.
Could logging controls be impacted by the change?		SME can test the logging controls by manually generating logs to ensure they were not affected by the change.
Could dial-up capabilities be impacted by the change?		SME can test the dial-up capabilities by doing a few test dials to ensure they were not affected by the change.
Could local accounts be impacted by the change?		SME can generate a list of local users and group membership and compare it with baseline.
Could the network diagram be impacted by the change?		SME can validate network diagram for accuracy and make any updates as needed.



EXHIBIT Q: PART 2.1 – MONITORING BASELINES FOR UNAUTHORIZED CHANGES (3RD PARTY TOOL OPTIONS)

The images below are screen shots of how a 3rd Party Tool may indicate a baseline attribute detected change. Screen shot #1 shows software has been modified as outlined by a red box. Screen shot #2 shows the detail of the modification. Notice the version number has changed.

Screen shot #1

Version	Severity	Version Type	Comment
May 17, 2018 11:06:58 AM		Current Baseline	Promoted by
Apr 20, 2018 11:00:12 PM	10,000	Modification	Promoted by
Sep 8, 2017 10:35:48 AM		Baseline	Promoted by
Sep 7, 2017 2:32:03 PM	10,000	Modification	Promoted by
Jun 4, 2017 11:47:39 AM		Baseline	

Screen shot #2

Sep 8, 2017 10:35:48 AM	May 17, 2018 11:06:58 AM
1	1
2 DisplayName DisplayVersion	2 DisplayName DisplayVersion
3 -----	3 -----
4 Nmap 7.60 7.60	4 Nmap 7.70 7.70
5	5
6	6

Legend: ■ Insertion ■ Deletion ■ Change



Revision Table		
Date	Version	Notes/Change
June 18, 2020	1.0	Initial Document

