2021 CIP Workshop Questions and Answers

October 2021

Table of Contents

Preface

In June 2021, Texas Reliability Entity, Inc. (Texas RE) hosted a Critical Infrastructure Protection (CIP) Workshop that included subject matter experts (SME) from across the ERO Enterprise, including representatives from: the North American Electric Reliability Corporation (NERC), the Electricity Information Sharing and Analysis Center (E-ISAC), ReliabilityFirst (RF), Western Electricity Coordinating Council (WECC), Midwest Reliability Organization (MRO), SERC Reliability Corporation (SERC), Northeast Power Coordinating Council (NPCC), and Texas RE. The session focused on Supply Chain, CIP-012, and CIP-008-6. Each topic featured a presentation on compliance followed by a panel discussion of its security aspects. The workshop's presentations along with a recording of the event are available.

Critical Infrastructure Protection
WORKSHOP
RF
TEXAS RE
WECC
SERC
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
NPCC, Inc.

During the workshop, attendees were encouraged to submit questions. Afterwards, all of the questions were compiled and the ERO Enterprise CIP SMEs collaborated on the answers contained within this document. If you require further clarification on any particular answer, please contact your Regional Entity's CIP Compliance team.

Supply Chain Compliance

Q: Is CIP-013-R2-L1-01 simply going to be the Procurement tab of the CIP Evidence Request Tool?

No, CIP-013-R2-L1-01 states. "*Provide a listing of persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services*."

Q: In R2, where it provides the exception rule that existing contracts/POs do not need to be redone for implementation...do you agree that any new (post 10/1) procurements under these pre-existing agreements need to follow your plan? or would all new procurements be exempt?

CIP-013 procurement(s) are not exempt if there is an existing contract/PO in place. Any procurements on or after October 1, 2020, associated with high and/or medium BES Cyber Systems are in-scope and Responsible Entities must implement their supply chain risk management plan(s) where applicable.

Q: Are there any known issues or concerns with regard to Electric Reliability Organization (ERO) endorsed guidelines for CIP-010-3 R1 Part 1.6, 1.6.1 verification of a software source? Have any issues or concerns been reported to NERC regarding CIP-010-3 software verification endorsed guidelines for 1.6.1?

The ERO Enterprise does not currently see issues with the guidance document; however, if there are known security vulnerabilities identified, then the Responsible Entity must demonstrate controls are implemented to validate the software verification.

Q: For new BES Cyber Systems, where the baseline has not been established yet, is all the new software required to be validated for software integrity?

It is incumbent on the Responsible Entities to have baselines established per Part 1.1. Per Part 1.6, "Prior to a change that deviates from the existing baseline configuration…"; the identity of the software source and integrity must be verified.

Supply Chain Security

Q: Do you have a feedback loop with opensource software vendors. If, when testing software, you discover vulnerabilities; is the reporting part of your security process?

If applicable, it is incumbent on the Responsible Entity to implement a feedback loop with open source software vendors. Responsible Entities are expected to mitigate and/or accept all identified risks as dictated by their Supply Chain Risk Management (SCRM) plan. Mitigation of all identified risks may include adding new controls or leveraging existing controls. Additionally, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and Electricity Information Sharing and Analysis Center (E-ISAC) are both good sources for reporting vulnerabilities.

Q: Who looks into backdoors coded into opensource software? The entity or the vendor?

CIP-013-1 requires Responsible Entities to identify and assess cyber security risk(s) to the BES for applicable vendor products or services, including open source software. Additionally, CIP-010-3 R3 vulnerability assessments may identify vulnerabilities like backdoors associated with opensource software.

Q: Can you contract the services to evaluate open source software, if you don’t have the team in place to evaluate the integrity of open source software?

Responsible Entities may contract services to identify and assess cyber security risks for open source software pursuant to CIP-013-1 R1, but it is incumbent on the Responsible Entity to document such services in the SCRMs. Specific to CIP-010-3 R1, Part 1.6, a Responsible Entity’s method, such as use of contracted services, to verify the identity and integrity of open source software must be documented in the configuration change management processes.

Q: Is Linux distribution considered “open source?”

Yes, a Linux distribution could be considered open source software and should be identified in a baseline configuration (CIP-010-3 R1, Part 1.1.1) and should follow all CIP-010-3 R1 processes (including Part 1.6). It may be difficult to confirm use of open source if it is embedded in another package.

Q: Given open source code is regularly used in commercial software applications and platforms, what is expectation for software bill of materials and subsequent assessment under NERC SCRM? How can that be achieved if vendors don't have the information? How can that risk be associated to risk to BES?

Per CIP-013-1, it is incumbent on the Responsible Entities to identify and assess cyber security risk(s) to the BES from vendor products or services. Responsible Entities are expected to mitigate and/or accept all identified risks as dictated by their SCRM plan. Mitigation of all identified risks may include adding new controls or leveraging existing controls.

Q: Does a third-party risk assessment vendor have any liability if they give an "all clear" signal to a customer and it turns out the software had malware and the party installing the software is severely impacted?

Liability discussions and contract agreements are between the Responsible Entities and the third-party risk assessment vendor.

Q: CIP-013, if relying on third party risk assessment of a vendor is used. What type of assessment of the third-party assessor would meet the compliance measure of the accessor being credible?

As there is no single approach that will work for all Responsible Entities, risk assessment should adequately identify and assess risks associated with the responsible entities' high and medium impact BES Cyber Systems pursuant to an entity's documented SCRM(s).

Q: SCRM of Operational Technology (OT)/Industrial Control Systems (ICS) risk does not directly equate to risk to BES. How will auditors take that aspect into account if a utility determines a high OT/ICS risk, yet minimal or no impact to BES if utility elects to accept or not mitigate the OT/ICS risk?

This should be documented according to the SCRM Plan, and other mitigating factors should be in place to minimize the accepted risk. Additional questions will be asked if there is just a blanket statement of accepting all risk from auditors.

Q: How much are you seeing SCRM with North American Transmission Forum (NATF) documents and what are the Regions' thoughts on the National Institute of Standards and Technology (NIST) Supply Chain, SP 800-161 Rev. 1?

The ERO Enterprise has seen both used for supply chain risk management plan(s).

Q: If an entity performs a pre-assessment of existing vendors, do they need to perform an additional risk assessment for each contract? How long is a preassessment good for?

Any procurements on after October 1, 2020, associated with high and/or medium BES Cyber Systems are in-scope and Responsible Entities must implement their supply chain risk management plan(s) where applicable.

The adequacy and timeframe of pre-assessments should be documented within Responsible Entities' supply chain risk management plan(s).

CIP-012 Compliance

Q: Regarding CIP-012 applicability to Generator Owners/Operators based on the current NERC definition of Control Center; we have one Medium Impact Control Center (with 1 primary, and 1 back up datacenter located off premise). Does CIP-012 apply if we only own/operate 1 Medium Impact Control Center?

If the backup data center meets the NERC definition of a Control Center, then data exchange protection could be applicable. It is incumbent on the Responsible Entity to document and maintain evidence demonstrating why or why not a backup data center meets the definition of a Control Center. Additionally, the identification of the security protection(s) used and where they are applied must be documented and implemented.

Q: If applicable, is the Control Center (Personnel and Workstations), or the Primary datacenter (cyber systems, and routers responsible for Inter Control Center Protocol (ICCP) traffic) the focus of identifying the requirements in the CIP-012 plan?

The primary focus of CIP-012 is about the data. Specifically, the data flow between Control Centers. Protection of Real-time Assessment and Real-time monitoring data between Control Centers, whether that is ICCP or any other type of data, which can take many forms. Determine where data protections are to be applied and what data protections make the most sense to ensure the CIP-012 security objectives are met. The security objectives of CIP-012 are currently to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data between Control Centers.

Q: Does CIP-012 include the communications between Control Center and backup control within the same entity? How about data that is used for backup Real-Time Contingency Analysis (RTCA)?

CIP-012 compliance includes both inter and intra entity transmission of sensitive data between Control Centers. This includes data exchange between a primary and backup Control Center.

The primary focus of CIP-012 is protecting data in transit between Control Centers. If data is being backed up to a Control Center, that process needs to be protected under CIP-012.

Q: Would this include communications between a backup Control Center and Control Center even if that backup control center is not always in use?

Both inter and intra entity sensitive data transmission protections should be implemented for CIP-012 compliance. This includes data exchange between a primary and backup Control Center. CIP-012 is about protecting data in transit between Control Centers, so protections should be in place for whenever data communications are occurring.

Q: Is Responsible Entity the same as registered entity?

Responsible Entity refers to the registered entities that are subject to the CIP Standards.

Q: Will the Joint Registration Organization (JRO) / Coordinated Functional Registration (CFR) be sufficient to identify the responsibilities of the different entities?

CIP-012 R1, Part 1.3, requires Responsible Entities to identify which security controls each party is responsible for to meet the security objectives. An agreement needs to show who is responsible for each applicable security control.

CIP-012 Security

Q: Some entities use remote terminal units (RTU) as 'mailboxes' to exchange real time data between control centers rather than ICCP. We view this as in scope for CIP-012 and the communication is in our data specification. How do the Regional Entities view this?

There is CIP-012 applicability for the exchange of Real-time Assessment and Real-time monitoring data between Control Centers regardless of whether or not it is ICCP. Types of communication can include, ICCP, Phasor Measurement Units (PMU), Operations Planning Coordinator (OPC), VME Based Remote Terminal Unit (VRTU), and any other protocol that meets the NERC definition. If the relationship falls under the NERC definition of Real-time Assessment and Real-time monitoring data between NERC defined Control Centers, then it is in scope for CIP-012.

Q: Would RTCA data from the BA CC to our System Operators be considered applicable to CIP-012?

If both the BA and the Entity's Control Center meet the NERC definition of a Control Center, then any Real-time Assessment data being transmitted between them would be in scope for CIP-012.

CIP-008-6 Compliance

Q: Is each applicable system type (high impact BES Cyber Systems, medium impact BES Cyber Systems, low impact BES Cyber Systems, high impact Electronic Access Control or Monitoring Systems and medium impact Electronic Access Control or Monitoring Systems) required to have an exercise per time requirements?

The Cyber Security Incident response plan(s) must be tested in accordance with CIP-008-6 R2, Part 2.1 and/or CIP-003-8 R2, Attachment 1, Section 4. If a Responsible Entity has two separate Cyber Security Incident response plans for CIP-008 and CIP-003, the expectation is to see the CIP-008 plan tested at least once every 15 calendar months and the CIP-003 plan tested at least once every 36 calendar months. If a Responsible Entity has a combined Cyber Security Incident response plan that covers low, medium, and high impact BES Cyber Systems, a single test every 15 calendar months would be adequate.

Q: Is a "read through" and discussion of items to update in an incident response plan with all stakeholders (those listed in the Roles and Responsibilities) acceptable to meet the testing requirement?

A “read through” is not identified as an acceptable testing method in CIP-008-6 R2, Part 2.1.

Responsible Entities are required to test each Cyber Security Incident response plan at least once every 15 calendar months using one of the following methods:
1) By responding to an actual Reportable Cyber Security Incident
2) With a paper drill or tabletop exercise of a Reportable Cyber Security Incident
3) With an operational exercise of a Reportable Cyber Security Incident

Q: CIP-008-6 4.1 Initial Notification - Can the notification be a copy of the DOE-417 form with all required information in R4?

Yes, the initial notification requirements specified in CIP-008-6 R4, Part 4.1 can be a copy of the DOE-417 form as long as all of the required information is captured in the form and the notification occurs within the timeframes detailed in CIP-008-6 R4, Part 4.2.

Q: How do Regional Entities recommend that an entity determine when the clock starts ticking for R4.1? Is a group analysis that determines a reportable or attempt to compromise appropriate?

The clock starts ticking for a Responsible Entity to perform initial notification once the determination has been made by the Responsible Entity that the Cyber Security Incident is either a Reportable Cyber Security Incident or an attempt to compromise a system identified in the “Applicable Systems” column for CIP-008-6 R4, Part 4.2. Gathering a group to perform analysis and make the determination is advisable.

Q: In the NERC Standard it specifically states National Cybersecurity and Communications Integration Center (NCCIC), I have done a lot of running around to get an email on where they get sent to, how do you keep up with the changes and will the NERC standard be updated with the NCCIC entity to send to/provide the email address to use for submitting the reports to?

Identifying the successor organization can be challenging due to organizational restructuring. Periodically checking the website or checking with E-SIAC would be a way to keep up with any changes. The reporting link is listed here.

If a revision were to occur to the Standard as a part of the Standards Drafting process, updates to outdated information would be updated accordingly.

Q: Is there not a revised DOE-417 that includes the attributes in R4.1?

Most recently, the OE-417 form was renamed and revised to the DOE-417 form. Keep in mind, the revised form does not require the functional impact, attack vector used, or the level of intrusion that was achieved or attempted to be submitted. However, the form does include instructions for users to include the Cyber Attributes in the narrative (Line T in Schedule 2).

Additionally, the revised form allows for a copy of the form to be sent to E-ISAC and DHS CISA or their successors, if the appropriate boxes are selected in Line W.

CIP-008-6 Security

Q: Why wasn't the 6-hour reporting timeline mentioned on slide 96 (1 hour and by the end of the next calendar day after determination was mentioned)? A 6-hour reporting timeline for a "Cyber event that could potentially impact electric power system adequacy or reliability."

The notification timelines mentioned in the presentation are specific to the notification requirements for CIP-008-6. The six-hour reporting timeline for a cyber event that could potentially impact electric power system adequacy or reliability is required for the DOE-417 form, not CIP-008-6. This type of cyber event may not rise to the level of a Cyber Security Incident that was an attempt to compromise an applicable system and/or a Reportable Cyber Security Incident. This information was excluded from the presentation to avoid confusion.

Q: How helpful is a paper drill? Why isn't the requirement to do an active assessment annually instead?

There are several benefits that a paper drill or tabletop can provide. For example, a paper drill familiarizes key personnel with their roles and responsibilities, the plan, and can help to identify procedural deficiencies. Active participation from all stakeholders and robust testing scenarios are essential to maximizing the benefits gained by a paper drill or tabletop.

Information related to the drafting of CIP-008-6 can be found at the link here.