A SANS Implementation Guide

Implementation Guide for Vendors and Integrators Working in NERC-CIP Environments

(Companion Piece to "How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet")

Written by **Tim Conway**

July 2020

Sponsored by:

Fortinet

Electric utilities around the world face numerous operational challenges and risks in maintaining system reliability and compliance. As electric utilities develop security control strategies to manage the risks of cyber and physical attacks, they need to consider people, processes and technology. Many of these risks extend to third-party organizations and need to be addressed in collaboration with multiple organizations working together toward a common goal.

A wide variety of organizations around the globe perform work with North American electric utilities. Suppliers of parts and services, construction crews, contractors, consultants, physical security protection professionals, automation controls systems engineers and cybersecurity vendors are all part of the diverse ecosystem that interacts with electric utilities in the performance of capital projects as well as the operating and maintenance tasks of ensuring reliability across the electric system.

Many of these third-party organizations also support electric utilities in other parts of the world or sectors outside of the electric industry. They may find it more challenging to do business with electric utilities subject to the North American Electric Reliability Corporation (NERC) Standards.[1] Working with a utility subject to the NERC Critical Infrastructure Protection (CIP) Standards may also seem confusing and inconsistent because one CIP customer may require completely different product or service capabilities than another customer subject to the same set of standards.

[1] www.nerc.net/standardsreports/standardssummary.aspx

This paper examines some of the essential NERC CIP Standards for third-party organizations to understand as well as how the requirements affecting third-party products and services may vary from site to site or organization to organization. Figure 1 shows how NERC CIP applies to third parties and entities.

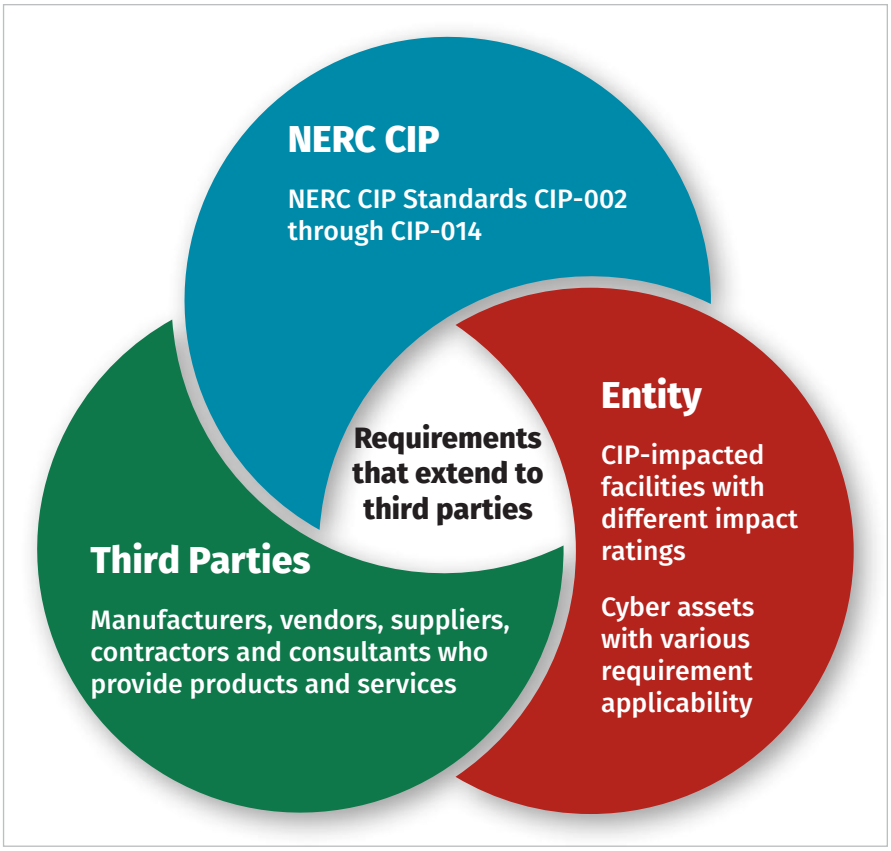

Figure 1. Venn Diagram of NERC CIP Applicability

NERC CIP is constantly maturing and changing. Personnel working for electric utilities with direct responsibilities to manage CIP programs may find value in reading other perspectives on the topic. NERC-registered entities are ultimately responsible for ensuring the reliability of the electric system and are also ultimately the ones responsible for maintaining compliance. Third-party organizations will not suddenly need to independently defend an approach during an audit. Neither will they need to debate the security benefits versus compliance benefits during an enforcement action with financial penalties on the line. Third-party organizations are important extensions of utility CIP programs from the perspective of governance, personnel, access, information, products and services. For these reasons, this paper addresses items of most interest to third-party organizations working in CIP-applicable areas from the following CIP Standards:

- CIP-003—Security Management Controls
- CIP-004—Personnel and Training
- CIP-011—Information Protection
- CIP-013—Supply Chain Risk Management

Third-party organizations are extensions of utility CIP programs from the perspective of governance, personnel, access, information, products and services.

Although the rest of the NERC CIP Standards are extremely important to organizations and possibly to third parties, the level of importance and relevance of those other Standards depend on the product or service offered by a given third party. This paper focuses on the CIP standards that should be understood as a baseline minimum regardless of the products and services offered. Third parties working in a NERC CIP environment need to understand the following:

- The CIP requirements as they apply to their products
- CIP requirements for their people supporting CIP-affected entities
- The CIP-applicable customer information protection requirements they interact with
- Their organization's obligations in relation to physical and electronic access to CIP assets

Consider the items listed as required knowledge or a cost of doing business for organizations that are providing products or services used in a NERC CIP environment. Third parties truly are an extension of an entity's overall CIP program and an extension of an organization's overall risk. An example of this can be seen in the US$2.7-million penalty incurred by an electric utility for a violation of the NERC CIP information protection requirements.[2] An independent information security professional identified sensitive NERC CIP–related data exposed in open source to the utility. The utility found that a third party had not properly protected the data and that the data had been exposed for 70 days. After these discoveries, the entity determined it needed to self-report the violation, which ended with a US$2.7-million assessed settlement penalty determination. Consider the risk organizations face as they think about the various third-party organizations in possession of project data or access to NERC CIP–related system files necessary for support purposes. Large vendors typically have document management systems with appropriate workflows and well-established data handling procedures. Often, these existing controls are equivalent to or better than the CIP information protection requirements. There are also very small organizations, however, that may provide specific services or consulting that do not have the capability to adequately track, classify and protect each piece of relevant data. Many third-party organizations may not even know they need to protect specific pieces of information under NERC CIP.

This paper presents approaches third parties can take to put their customers first and to take seriously their role as an important extension of their customers' CIP programs.

Note: NERC uses specific terminology that has defined meaning in the context of its protocols and rules. Because NERC capitalizes that terminology, this paper often follows that convention to preserve NERC's definitions.[3]

Product and Service Offerings

Imagine a vendor attending a product meeting and telling the CIP team, "Thanks for coming. Our team has done some research, and we see your entity has these specific NERC registrations and performs these particular functional obligations. From what we can tell, you would likely have these types of assets and are probably facing some big challenges in the following standards. We would love to hear details of your unique program implementations before we show you where our product has helped some of your peers with similar cybersecurity and compliance challenges." Your CIP technical practitioners and CIP compliance analysts would not only be floored, but also would be able to move forward immediately with some level of confidence that the third party had a necessary level of knowledge to positively assist with your needs.

Instead, most meetings start with the third party asking the customer to "explain this whole CIP thing" and often end with, "You are the only customer asking for that."

---

[2] "Data Exposure by Vendor Leads to $2.7 Million NERC Penalty for Utility," www.morganlewis.com/pubs/data-exposure-by-vendor-leads-to-2-7-million-nerc-penalty-for-utility

[3] "Glossary of Terms Used in NERC Reliability Standards," www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

In fairness, the industry has come a long way with solution offerings relevant to the CIP standards. Both sides of the discussion need to continue to progress, though. Entities need to better understand the vast amount of security products, technologies or features currently available. They also need to learn how to leverage them for cybersecurity benefits in a way that does not create CIP compliance conflicts or concerns. Likewise, third parties need to immerse themselves in the complexities of the CIP standards and bake that knowledge into products and solutions.

As third parties examine their offerings, they need to understand the variability of the standards and existing requirements based on the asset's impact rating. In the old days of CIP (versions 1–3),[4] there was a one-size-fits-all approach whereby something was either in the CIP program or it wasn't. In today's CIP program, wild variations of applicability affect which capabilities are necessary depending on many conditions. Ultimately, the higher risk-impact-rated facilities and assets are subject to the most requirements, whereas facilities facing medium impact are subject to a large majority of the requirements but not all, and the low-impact areas are subject to only a few of the requirements. This information exchange will occur through a series of questions to and from customers, as presented in "Questions for Vendors to Ask and to Answer."

Many product and service providers focus their NERC CIP efforts on the alignment of their product offerings compared to NERC CIP Standards and Requirements. Typically, these requirement-to-capability matrices are offered up as one-page marketing sheets for potential customers to see at a glance how the various solutions meet the requirements. Many of these product matrix sheets are simply a reference to a product category, not necessarily an effort to align a product's capability with an entity's CIP compliance program. The unfortunate result is a gap between how solution providers believe they align with CIP and what utilities need to enhance their CIP programs. This gap may cause entities to perform exhaustive, time-consuming CIP product evaluations with limited resources. It may even cause them to make selections based on product documentation, discovering limitations after purchase. This disconnect is an ongoing challenge for utilities performing these product assessments across multiple CIP projects or integrating solutions into ongoing CIP programs for maintenance and continuous program improvements. Meanwhile, vendors and manufacturers try to keep up with a dynamic set of NERC CIP regulations—all while managing these challenges across a wide variety of customers with various interpretations of NERC CIP Standards.

Questions for Vendors to Ask and to Answer

Ask customers these questions in regard to product offerings:

1. Where is the product?
2. What impact rating (High, Medium, or Low) does the facility or asset where you will be using the product have? Is there any way to lower the impact rating and reduce requirements and liability?
3. What is the product doing?
4. What product features will you be using, and what classification is the product: Bulk Electric System Cyber Asset (BCA), Protected Cyber Asset (PCA), Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Transient Cyber Asset (TCA)?
5. How is the product being used?
6. What communication methods will you be utilizing: External Routable Connectivity (ERC), Interactive Remote Access (IRA) or Dial-up? If none of these, will there be an Electronic Security Perimeter (ESP)?

Be prepared to answer these questions from customers:

1. Does the product do what it needs to? Demonstrate the specific capabilities required of the product based on how the customer is intending to implement it.
2. Will it work for an organization? Provide examples or walk through how the product will integrate into a CIP program in a manner that helps maintain continuous compliance and necessary security features.
3. How will the product help in an audit? Consider the product reporting capabilities, logs or audit trail that will assist an entity in satisfying auditor data requests for evidence of compliance throughout the multiyear audit period. This proof is important for solution providers to understand; consider not only the immediate customer security and compliance needs, but also the future ability to demonstrate that those features were implemented.

[4] "Inactive Reliability Standards," www.nerc.com/pa/Stand/Pages/InactiveReliabiltyStandards.aspx?jurisdiction=United%20States

The NERC CIP Standards are a set of requirements targeting what needs to be achieved. They are not prescriptive about how a requirement needs to be met, which allows entities to design their own approaches—but it results in more than one way to achieve compliance, leaving the door open for interpretation issues and potential pitfalls. Entities, vendors and manufacturers alike can seek guidance and work together in a number of ways to reduce confusion regarding product capabilities and CIP applicability, as detailed in Figure 2.

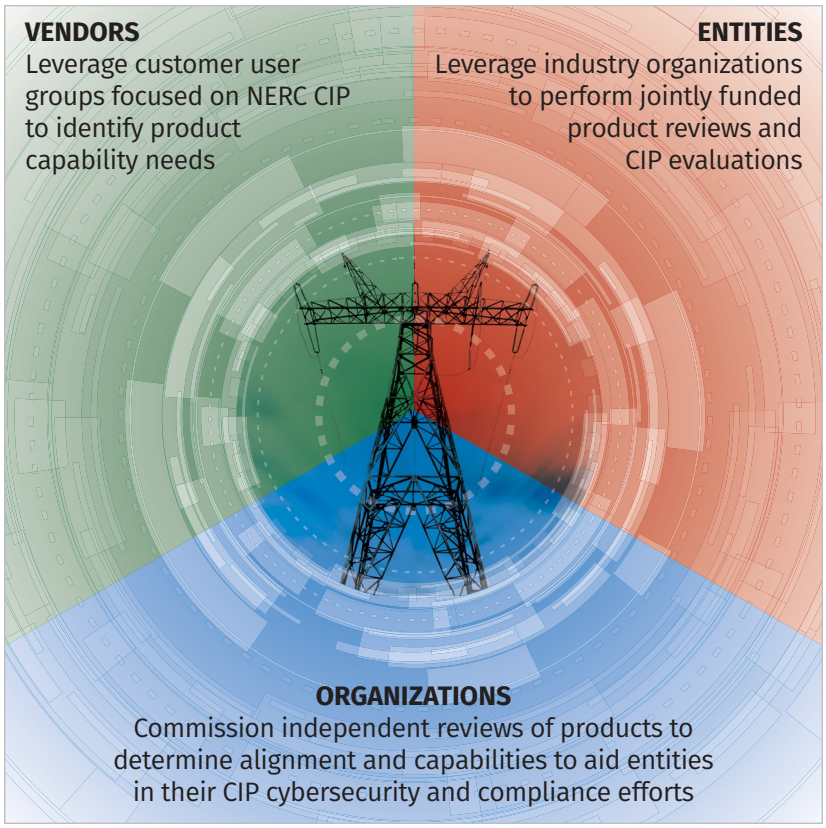

Figure 2. How Entities, Vendors and Manufacturers Can Work Together to Meet NERC CIP Standards

There have been calls from industry to develop a "CIP-certified" product testing or validation organization or process similar to UL or EnergyStar. Some vendors claim to be selling CIP-compliant products. Either of these concepts, if they existed, would address only the capability to configure a product to align with the CIP requirements—they would not address the evidence requirements for configuration, management, operation or documentation. All these items need to be taken into account. The only sustainable approach is for asset owners and operators to work closely with their third-party organizations and make sure everyone understands that CIP is a team sport.

Now that we've covered product or service capabilities, it's time to look at how third parties should be prepared to integrate into entity CIP programs.

CIP-003 Security Management Controls

CIP-003 (Security Management Controls) establishes the overall CIP program governance structure. Nine required policies exist within CIP-003 pertaining to High- and Medium-impact facilities and assets. These nine policies must address the following topics:

- **1.1** Personnel and training (CIP-004)
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access
- **1.3** Physical security of BES Cyber Systems (CIP-006)
- **1.4** System security management (CIP-007)
- **1.5** Incident reporting and response planning (CIP-008)
- **1.6** Recovery plans for BES Cyber Systems (CIP-009)
- **1.7** Configuration change management and vulnerability assessments (CIP-010)
- **1.8** Information protection (CIP-011)
- **1.9** Declaring and responding to CIP Exceptional Circumstances

CIP-003-8 contains six policies that must address the following items for Low-impact facilities and assets:[5]

- **1.2.1** Cyber security awareness
- **1.2.2** Physical security controls
- **1.2.3** Electronic access controls
- **1.2.4** Cyber Security Incident response
- **1.2.5** Transient Cyber Assets and Removable Media malicious code risk mitigation
- **1.2.6** Declaring and responding to CIP Exceptional Circumstances

Third parties are responsible for understanding how these policies affect their solutions and personnel. Accordingly, they should also be familiar with the latest versions of the standards and requirements, and their customers' policies relevant to CIP. To ensure compliance with the requirements, registered entities may provide training and require policy review attestation documents for third parties to sign. Third parties also need to know how to access document management systems in which the policies reside. Organizations are responsible for ensuring that CIP training references internal policies with functioning links so third parties aren't forced to accept the policies sight unseen. Both sides need to treat this sharing of information as more than a compliance check box.

Present the information sharing like you would a safety program. Provide guidance on how work is done throughout various environments of differing risk to personnel.

If you were to enter an electric utility facility, you would likely need to go through safety training. Most of us would consider this training a necessary step to avoid injury. You would likely ask questions about the environment to ensure you didn't do anything to put others in harm's way. You'd ask about your responsibilities if an event occurred or verify actions you might need to take to ensure personnel safety and protection of the facility.

In this same manner, third parties and service providers need to move beyond the basic required CIP training and move toward an understanding of their role in contributing to a sound CIP program that ensures safety of systems, reliability of the Bulk Electric System and the integrity of our critical infrastructure. Take the policy review seriously; if the process is lacking, ask the utility to do better.

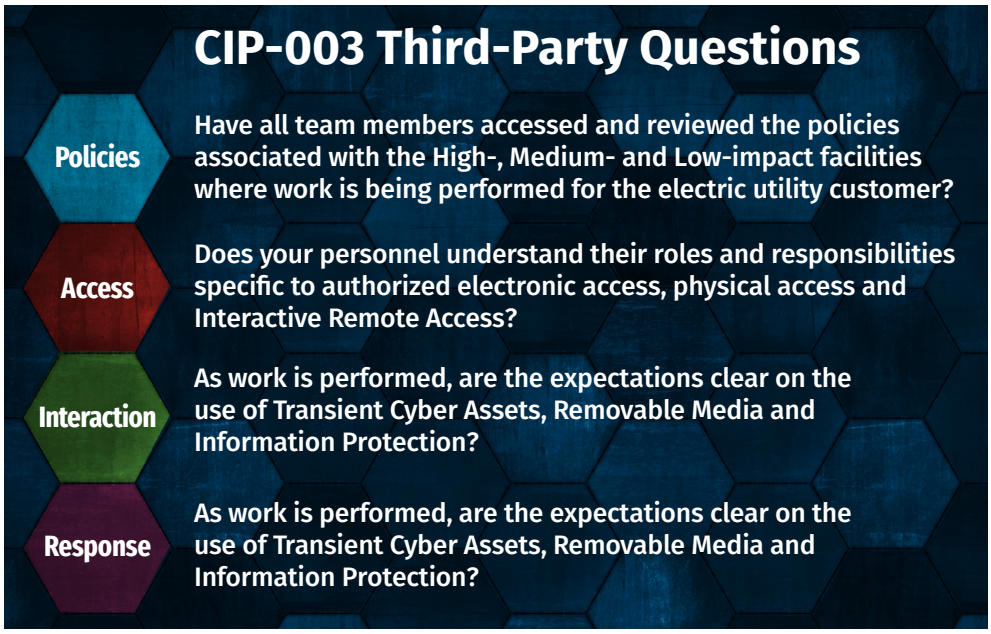

Figure 3. Summary of CIP-003 Areas of Focus for Third Parties

CIP-003 governance approaches vary, and third parties are faced with the complexities and variances across a multitude of customers. Nevertheless, third parties need to be able to access and quickly reference a policy when needed for a particular customer. In addition, third parties should anticipate unique approaches for each utility customer to address the required CIP-003 policies. Figure 3 summarizes the questions related to CIP-003 that third parties should ask.

[5] The requirements applicable to Low-impact facilities and assets continue to grow, and include CIP-002, CIP-003, and CIP-012

CIP-004 Personnel and Training

At first glance, the CIP-004 standard seems to be merely a training standard, but it contains multiple programmatic elements, including:

- Training requirements pertaining to security awareness and specific training topics of record for individuals with access
- Personnel Risk Assessment (PRA) requirements addressing background check performance and processing
- Access control requirements and access granting based on need with periodic reviews of approvals as well as actual access rights in place
- Access revocation requirements pertaining to personnel transfers or terminations

The following review of these requirements will highlight the areas of greatest noncompliance and security risk associated with third parties.

CIP-004 Requirement 1

CIP-004's Requirement 1 specifies the need for a quarterly security awareness program that applies to individuals with authorized electronic or authorized unescorted physical access to BES Cyber Systems. (Third parties may be included in this scope.)

With this requirement, consider the balance between performing work with eased restrictions versus the added compliance and security risk of having unescorted access or electronic access. Say a third party needs to send personnel to a CIP site to perform work. While there, personnel are physically escorted everywhere and never allowed to directly interact with a CIP asset. They would not be subject to these CIP-004 requirements because they have not been granted authorized access. Depending on the nature and duration of the work being performed, it can be a rather painful and unproductive experience for all involved to provide continuous escorts and perform actions on a CIP asset working with a third party rather than allowing the third party to directly perform the work. It may be tempting to just provide the individual with authorized electronic or authorized unescorted physical access to BES Cyber Systems, but certain requirements must be satisfied to gain access and maintain access. Third parties shouldn't skimp on making sure those requirements are met.

A life cycle of requirements applies while the individual maintains access, in addition to the entangled requirements for how they interact with the CIP assets. There are also requirements related to removal of their access. Requests for access should not be taken lightly by third parties, and denial of access should not be viewed negatively. The entities are simply managing security and compliance risk along with operational needs. Third parties should lead this conversation about limiting the scope of personnel that would potentially need access to limit risk. They should also have discussions about managing the contractual support cost of having large numbers of personnel undergoing periodic training requirements to support the customer in this effort to balance risk. If a third party seeks to limit the number of in-scope personnel with access, it must have a strategy in place for an emergency requiring a potential surge capability of personnel. Work with the entity to understand its approach to CIP Exceptional Circumstances and incident response actions.

CIP-004 Requirement 2

The second training requirement applies across nine training topics including training to the nine policies mentioned in CIP-003. Here, too, many organizations have customized training approaches that vary greatly, from emailed PowerPoints to instructor-led training and assigned learning management system modules. As you encounter these training programs, you will find some training programs that repeat the language of the standards and point to CIP policies that simply reflect the language of the standards. For example, a requirement may say to provide a "continuous visitor escort;" the resulting policy states, "We will provide a continuous visitor escort," but discloses no details about how this will be managed or handled by the entity. For these types of training programs, third parties should seek additional guidance as they perform work to understand what requirements apply to which devices and what internal procedures are in place to govern the work being performed. The stronger the training program and more specific the policies are in regard to how an entity has implemented its CIP program, the clearer the expectations are to the third party performing the work. A vague and immature training program may satisfy strict compliance with requirements but may also introduce higher levels of security and compliance risk.

CIP-004 Requirement 3

Requirement 3 addresses Personnel Risk Assessments. It outlines the need to confirm the identity of the individual, perform a seven-year criminal history records check if available and establish a process to evaluate findings. This is a complex task that has to take into account a variety of concerns regarding country or state laws protecting personal information, limitations of using credit agencies to verify identity and numerous conflicts with employment laws and bargaining unit agreements (see Figure 4). This requirement presents an important issue for third parties: Their employees are their responsibility, and they must navigate all applicable laws governing that relationship. When performing work with a CIP entity, third parties must perform personnel background checks in accordance with customer requirements. They must also be able to provide the necessary

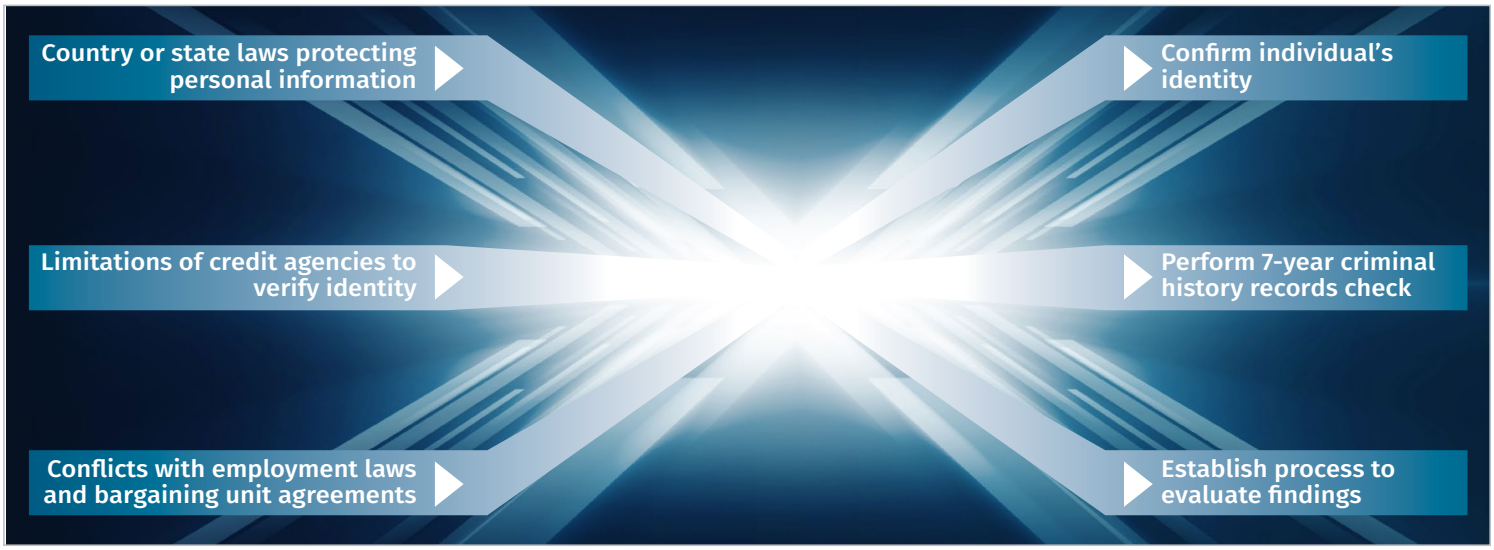

Figure 4. Elements of CIP-004, Requirement 3: Personnel Risk Assessments

attestations or evidence to support their processes and ensure their review efforts are in line with their CIP customer requirements. For third parties, these efforts would ideally be coordinated across a customer CIP focus group to ensure that the process satisfies or exceeds all CIP customer program requirements. When verified with CIP customers, it would be an excellent industry-leading effort to ensure the six NERC regions are in agreement with the approach.

In an ideal world, this element of CIP program maturity would progress to a NERC- or FERC-led credential establishment process in which individuals could take generic training and undergo a federal equivalent Personnel Risk Assessment (PRA), which would grant a CIP-eligible work permit. Entity-specific training requirements would address policy and site-specific details, but a more comprehensive training program could address the common elements that exist across utilities (similar to the approach being administered by the Transportation Security Administration [TSA] for port workers under the Transportation Worker Identification Credential [TWIC]). For now, without an agreed-upon CIP worker program in place for North America, third parties will need to continue customer-specific training programs and possibly multiple PRAs depending on customer requirements.

CIP-004 Requirement 4

As we move into the access control requirements within CIP-004, we start looking at the ongoing obligations of third parties to determine personnel needs for access to physical locations, electronic access to CIP assets and access to CIP-protected information. Assessing these access needs is not a one-time task; rather, it is an ongoing compliance task requiring access requests and approvals as well as reviews of access capabilities in effect compared to access rights that should be in place. This access control program is important for third parties to understand because they may wish to use shared accounts for tasks or have generic support accounts that are utilized by a group of individuals who all could be called upon to respond to customer requests. The training requirements apply to each individual—if a shared or support account is utilized, there is no tracking to prove all individuals with access to those accounts were also verified for access approvals, training and PRAs, and tracked for changes and revocations. This is why it's important to limit those providing support to CIP customers to dedicated, named individuals. If customer support requirements mandate more personnel be included in the scope, ensure the acceptance of potential compliance risk in managing a broader program.

By understanding the entity obligations to perform quarterly reviews of access authorization records and verification of access privileges every 15 months, third parties can consider the types of processes they can enable in their own HR systems to identify CIP-applicable personnel. Additionally, they can ensure workflow is capturing current job roles, customers are supported and associated PRA/training records are being archived in case a customer needs to rely on them in an audit.

CIP-004 Requirement 5

The last item within CIP-004 considers access revocation actions. Again for "personnel with authorized electronic or authorized unescorted physical access to BES Cyber Systems," specific triggering events create a need for timely action. If the triggering event is a personnel job transfer or reassignment, then the individual's physical and electronic access needs to be removed by the next calendar day, and the default accounts they had access to need to be changed within 30 days. If the triggering event is a termination action, then the individual's physical access and Interactive Remote Access need to be removed within 24 hours of the event, followed by removal of access to CIP BES Cyber System Information (BES CSI) by the end of the next calendar day and modification of default accounts within 30 days.

These requirements make it very challenging for entities to manage a program with zero deficiencies. The largest challenges often come from third parties who are not aware of the obligation to notify their customers of one of these triggering events. A security awareness email to all personnel with access, followed by a number of undeliverable emails to vendors and contractors, may be the first notice customers receive of an individual no longer with an organization. Discovery events like this happen frequently and result in potential violation self-reports, all because a third party did not notify the customer in an appropriate timeframe. Third-party organizations absolutely need to integrate specific access revocation procedures as well as customer notification workflow within their HR processes to ensure CIP-applicable entities can take the required actions to maintain compliance.

The largest challenges often come from third parties who are not aware of the obligations to notify their customers of certain triggering events.

Many third-party organizations don't take the CIP-004 requirements seriously enough: "We already do background checks on our new hires, and the training stuff is basic general knowledge that we just need to click through or say we looked at." In reality, CIP-004 is a set of complicated customer-specific obligations that third parties need to integrate into their own HR systems. They need to ensure the culture of compliance is well understood by all personnel supporting CIP entities.

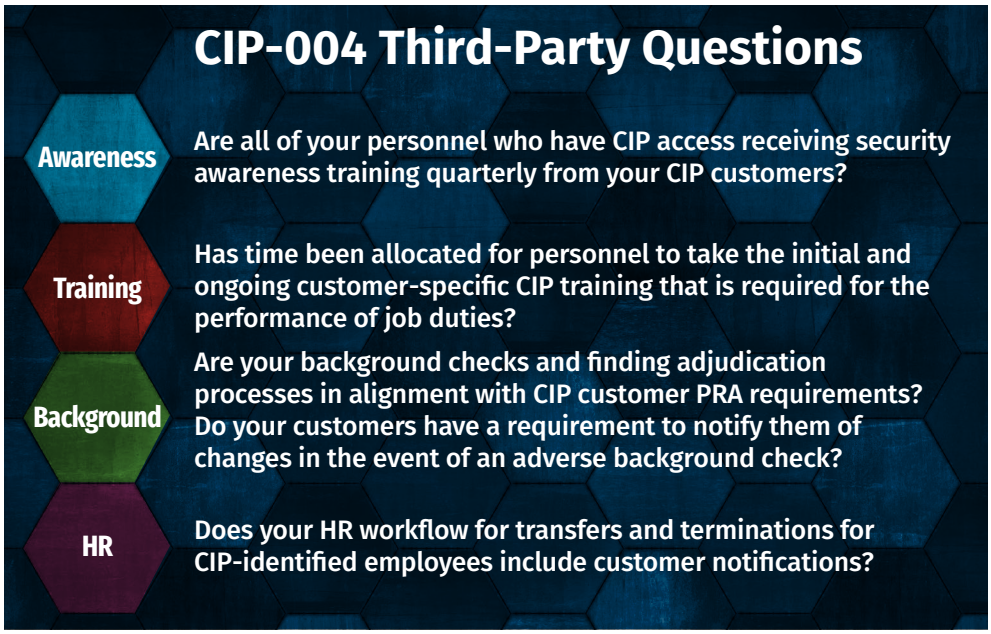

Figure 5. Summary of CIP-004 Areas of Focus for Third Parties

Figure 5 summarizes the questions related to CIP-004 that third parties should ask.

CIP-011 Information Protection

The information protection requirements of NERC CIP have been a complicated mix of changing rules across the maturing CIP standards. They've been further complicated by the nature of a growing data set located in an ever-increasing list of disparate locations. In the old days of NERC CIP versions 1–3, the requirements to identify, classify and protect information associated with Critical Cyber Assets existed as a requirement within CIP-003. The scope pertained to "at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information." There was no previous scoping of the information context or what could be done with it. This omission led to confusion and considerable constraints about what information could be shared with third parties for system specifications, maintenance procedures, work procedures, equipment inventories or even physical plans for construction crews. Annual assessments of program effectiveness and adherence needed to be performed, which was difficult to do in accordance with information that may have existed at numerous third-party organizations.

As the CIP standards matured and a new standard was created in relation to information protection, CIP-011 provided some important guidance in relation to scope of information classified as BES Cyber System Information. BES CSI is defined as "Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."

Equally important to understand is the language in the definition that provides guidance on what is not BES CSI: "BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements."[6]

To provide additional clarity, the definition also includes examples to consider as individual records are reviewed: "Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System."

Third-party organizations have within their possession a treasure trove of information related to system specifications, maintenance, implementation, support documents and other procedures, so these third parties must understand how that information should be classified, protected and disposed of when appropriate. Third-party organizations are

[6] "Glossary of Terms Used in NERC Reliability Standards," www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

not the information classifier and do not determine whether something is BES CSI. The registered entity to which the information is associated makes the BES CSI determination. Third parties should access CIP BES CSI on entity-provided storage locations and ensure employees are not saving local copies of the protected information. Remember, CIP information protection requirements pose a financial risk to utilities. Depending on contract liability language, they may also be of financial risk to third-party organizations.

Many CIP entities are establishing CIP contracts with third parties to establish a shared liability when assessed compliance violations are issued and the CIP entity feels that the root cause of the violation was linked to actions by a third party. When violations caused by third parties occur, the third party may incur financial risk it needs to manage. Third parties need to establish processes to limit the CIP BES CSI it has under its control. Instead of maintaining local copies of information, third parties should pursue the viability of accessing the information through approved methods on the customer site. Consider all the places this data could exist, with many people working on projects or utilizing email or file sharing applications to share data between companies. With growing numbers of those services leveraging cloud-based resources, it becomes a significant challenge to address the issues without formal policies and training relating to data exchange practices.

Information protection has been a difficult problem to manage since the beginning of CIP. Progress has been made over the years, but the nature of the challenges has continued to grow, requiring focused joint efforts from entities and third parties.

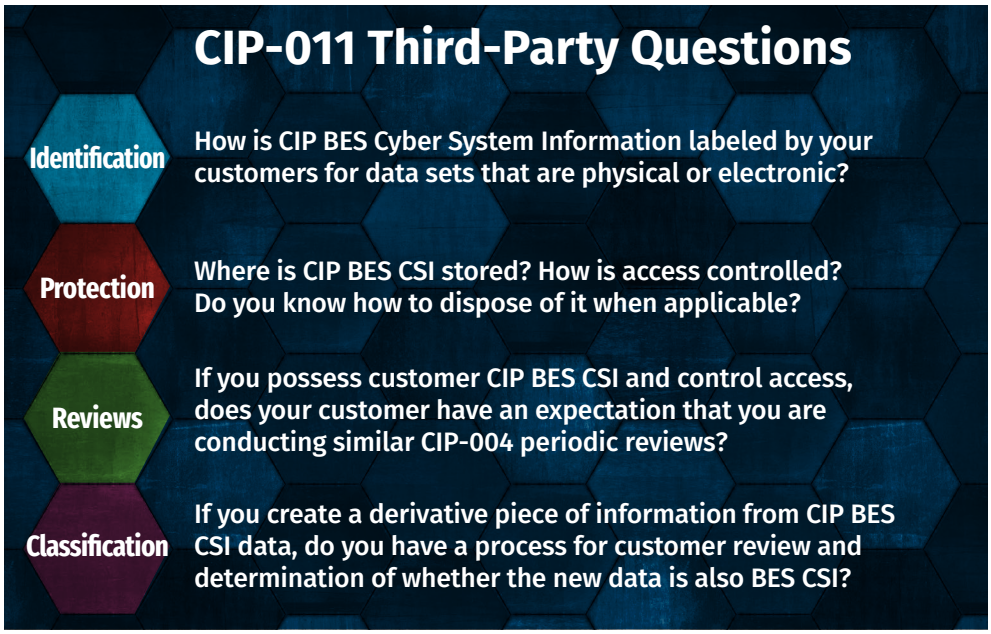

Figure 6. Summary of CIP-011 Areas of Focus for Third Parties

Figure 6 summarizes the questions related to CIP-011 that third parties should ask.

CIP-013 Supply Chain Risk Management

CIP-013 is a new standard and a first step in what will certainly be a long journey to address supply chain risk-management issues. CIP-013 brings the standards and requirements as close to the front door of third parties as possible. NERC and the regions do not have federal delegated authority to audit third parties and enforce mandatory standards or impose penalties. Their authority relates to NERC-registered electric utilities.

Therefore, the requirements of CIP-013 focus on the actions entities need to implement within their procurement processes to include language addressing:

- Vendor notification of incidents
- Coordination of response to vendor incidents
- Notification of remote or on-site access revocation
- Vendor vulnerability disclosure
- Verification of software integrity and authenticity
- Coordination of controls for vendor IRA and system-to-system remote access

Third parties should anticipate this language appearing in contracts and should be working with customer working groups to develop acceptable language and policies that satisfy the requirements. This collaboration would take the form of third-party companies sharing customer notification policies with their CIP customers to ensure they meet expectations. In addition, CIP customers should confirm the actions and expectations of what is to be performed if an incident occurs. Lastly, customer response actions need to be coordinated and may include additional CIP-008 notification requirements and revocation of third-party remote access. Notification also includes policies that provide details of vulnerability disclosure procedures, software verification and integrity testing procedures, and any controls in place for system-to-system communications. In many instances, third-party organizations are engaging in practices relevant to each of these items, but the procedures may not be mature or the policies formal enough to be shared with customers. This situation needs to be acted upon quickly, because entities will begin requiring this language in future contracts, and evidence of these capabilities will be required from CIP customers. Third-party organizations are encouraged to work with customer advisory groups, industry organizations like EEI (Edison Electric Institute) that have developed procurement language templates, and NERC regional entities to discuss evidence evaluation approaches that would help an entity satisfy CIP-013 audit requests.

Third parties should be working with customer working groups to develop acceptable language and policies that satisfy the requirements.

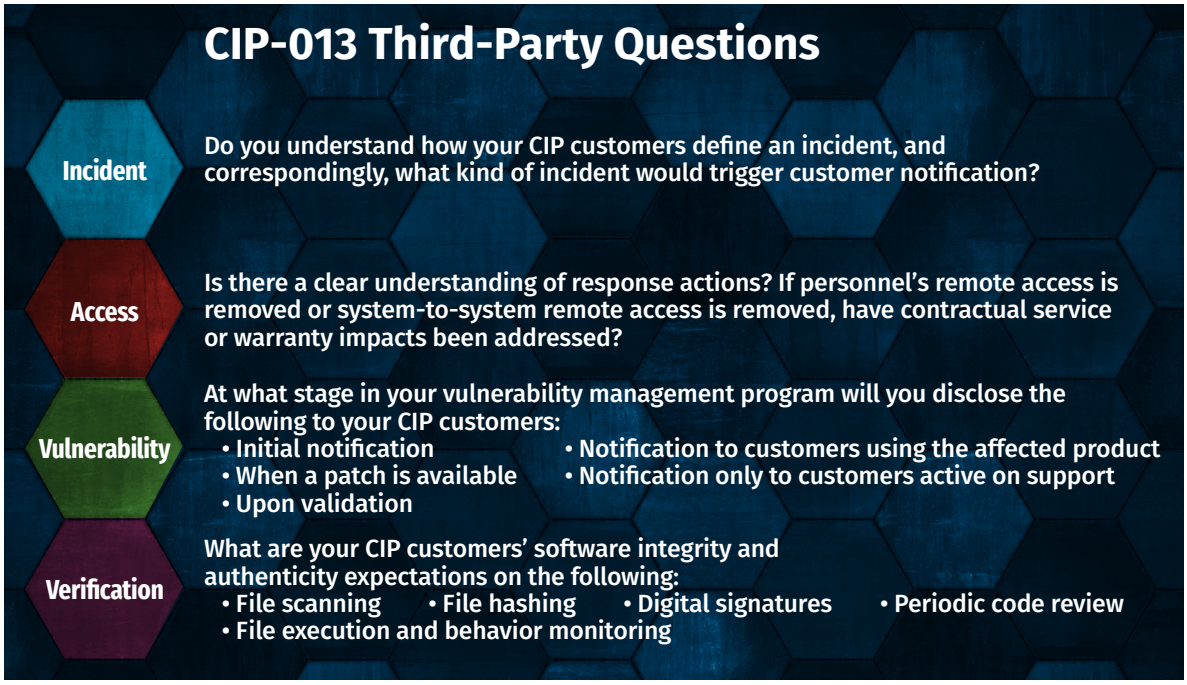

Figure 7. Summary of CIP-013 Areas of Focus for Third Parties

This is a new standard that will likely expand in scope to additional assets, then expand in scope with regard to requirements. Entities and third-party organizations need to move forward on CIP-013 quickly—it is highly likely that additional changes and requirements will be coming soon.

Figure 7 summarizes the questions related to CIP-013 that third parties should ask.

Conclusion

Too often, NERC-registered entities have managed the nuances of CIP programs on their own, without full involvement from their product and solutions providers. Entities viewed compliance as secondary or tertiary for third parties depending on how many of their customers were CIP-regulated. As utilities continue to expand and integrate third-party organizations at all levels of their CIP programs, they more commonly expect more and ask more of their third-party organizations. As critical infrastructure attacks targeting utilities through affiliated organizations become more common, we need to demand more from all stakeholders involved.

The CIP community has grown, and many product and solution providers have developed CIP expertise. Third parties have earned an important seat at the table to have their concerns and recommendations heard. NERC does not distinguish between an employee with access and a contractor with access, and adversaries do not discriminate between parties or care about regulations. If the risks to critical infrastructure apply to utilities as well as third parties, then the actions to protect the system apply equally as well.

About the Author

Author **Tim Conway** serves as the Technical Director for ICS and SCADA programs at SANS and is responsible for developing, reviewing and implementing technical components of the SANS ICS and SCADA product offerings. Recognizing the need for ICS-focused cybersecurity training throughout critical infrastructure environments and an increased need for NERC CIP hands-on training, Tim co-authored and instructs ICS456: Essentials for NERC Critical Infrastructure Protection. During his career, Tim has served as the chair of the RFC CIPC, the NERC CIP Interpretation Drafting Team, the NERC CIPC GridEx Working Group, and the NBISE Smart Grid Cyber Security panel.

Sponsor

SANS would like to thank our sponsor for this paper:

FORTINET®