North American Transmission FORUM

Community Confidentiality Candor Commitment

ERO Enterprise Endorsed Implementation Guidance

NATF CIP-013-1 Implementation Guidance

Version 2.0
Approval Date: 4/3/2019

Introduction

NERC "Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [or requirement within a Standard] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard."[1] This NATF Implementation Guidance document describes one way that a registered entity could comply with CIP-013-1 Requirement R1 and, subsequently, CIP-013-1 Requirement R2.

Reliance on Independent Assessments of Vendors as an Acceptable Means of Identifying and Assessing Vendor Risk

The ERO has endorsed the practice of a Responsible Entity obtaining an independent assessment of the vendor's production of BES Cyber Systems and/or related services as a means of complying with CIP-013-1.[2] The "Implementation Guidance for CIP-013" recommends that an entity's risk assessment process to identify and assess potential cyber security risks include "potential risks based on the vendor's risk management controls." Responsible Entities may consider assessing vendor risk-management controls though obtaining a "*summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations*."[3]

Responsible Entities that review independent assessments of vendors also build on the ERO-endorsed practice of relying on the "work of others" as a means of obtaining reasonable assurance that defined reliability and security objectives are being met by vendors. The "ERO Enterprise Guide for Internal Controls"[4] promotes ERO Compliance Enforcement Authorities evaluating the independence, capabilities, and competencies of the "work of others" (i.e., disinterested third parties or departments that are independent from the department performing a reliability function) for purposes of compliance monitoring.[5]

Just as the ERO may rely on the "work of others" to assist in determining how to monitor a registered entity's compliance, Responsible Entities, in the context of managing their supply chain risk, may rely on qualified independent assessments of a vendor's risk-management controls to demonstrate that it has assessed cyber security risks associated with the vendor's BES Cyber System.

Following the steps described below builds on the Implementation Guidance for CIP-013 to provide clarity on how the Responsible Entity may meet the obligations in both R1 and R2 when using an independent assessment, but does not obligate a Responsible Entity to choose an independent assessment under any particular set of circumstances.

[1] NERC Compliance Guidance Policy, November 5, 2015, *available at:* https://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

[2] Implementation Guidance for CIP-013-1 at p 4 (June 2017), *available at:* http://www.nerc.com/pa/comp/guidance/Pages/default.aspx.

[3] Implementation Guidance for CIP-013-1 at p 4 (June 2017), *available at:* http://www.nerc.com/pa/comp/guidance/Pages/default.aspx

[4] http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf

[5] Id. at Section 2.2.2.

Using Independent Assessments of Vendors

When Developing the Cyber Security Supply Chain Risk Management Plan, the Responsible Entity Describes Option for Relying on Independent Assessment (CIP-013-1, R1)

The Responsible Entity develops its Cyber Security Supply Chain Risk Management Plan(s) to address CIP-013 requirements. The Plan includes the Responsible Entity's process for assessing risk in procuring and installing BES Cyber Systems and transitioning from one vendor to another vendor. To incorporate reliance on independent assessments of vendors, a Responsible Entity's cyber security supply chain risk management plan, as required in CIP-013-1 R1, describes the Responsible Entity's process to:

1. ask vendors to provide an independent assessment (including a description of the methodology for performing that assessment), from an auditor[6], that evaluates the vendor's controls and tests specific control activities to meet, at a minimum, the criteria identified in CIP-013-1 R1 part 1.2 (see Attachment A);
2. evaluate the auditor's qualifications and cyber security framework used to perform the vendor assessment, ensuring that the third-party assessment is performed by auditor(s) with appropriate independence, credentials, and sufficient understanding of cyber security supply chain risk in the electric industry;
3. evaluate the scope and the results of the third-party, independent assessment;
4. document its evaluation of the independent auditor's qualifications, the methodology and scope of the review, and conclusions to determine what existing or additional mitigating actions are appropriate to manage risk; documenting those mitigating actions. (Note: Mitigating actions may include physical controls, logical controls, or contract modifications to address risk.)

In this way, the third-party assessment is made part of the entity's overall process used in procuring BES Cyber Systems that addresses each of the security issues listed in Part 1.2 of Requirement R1.

Using an Independent Assessment as a Means for Implementing the Cyber Security Supply Chain Risk Management Plan (CIP-013-1, R2)

For those BES Cyber Systems and/or related services for which the Responsible Entity has determined that it is appropriate to obtain an independent assessment, the Responsible Entity may show that it implemented its Plan as required in CIP-013-1, R2 through documenting that it:

1. asked for and received a third-party, independent assessment, and documented its conclusion that the independent assessor was appropriately qualified;
2. reviewed and confirmed (such as by using a predefined checklist) that the results of the third-party, independent assessment address the topics in CIP-013-1 R1.2;
    - **Attachment A** summarizes minimum criteria a Responsible Entity may use to review the third-party assessment. (It also provides additional criteria a Responsible Entity might consider.)

[6] Auditors providing independent assessments have appropriate credentials to provide such an assessment. For examples of appropriate certifications, see pages 134 – 137 of https://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/NERC_Compliance%20Monitoring%20and%20Enforcement%20Manual_v4_0.pdf for example qualifications. Other examples of relevant credentials include Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), and similar security and controls auditing certifications.

- **Attachment B** provides a predefined list of examples of known security frameworks that address the security topics specified in CIP-013-1, R1.2.

3. reviewed and evaluated the results of the third- party, independent assessment to confirm that vendor and/or Responsible Entity actions and security controls mitigate the cyber security risks to procure the BES Cyber Systems. This step includes using the third-party assessment to inform the actions the entity takes to address the security issues listed in Part 1.2 of Requirement R1.

As the Responsible Entity is ultimately responsible for compliance with the Cyber Security Supply Chain Standards, the Responsible Entity maintains evidence to demonstrate its compliance to CIP-013, including documentation of its Cyber Security Supply Chain Risk Management Plan and completion of recurring reviews as well as use of its Cyber Security Supply Chain Risk Management Plan. Use includes identifying risks, risk assessment conclusions, and mitigating actions and status.

Attachment A – Cyber Security Criteria

At a minimum, entities assess whether their vendor(s) can meet basic security criteria.

Notification/Recognition of Cyber Security Incidents

Vendors need to be able to identify when an incident occurred to ensure that the vendor can notify the entity in the case of such an incident. To meet this requirement, the vendor may have aligned with numerous cyber security frameworks (see table 1 in attachment B).

Coordination of Responses to Cyber Security Incidents

Vendors should coordinate with the entity their responses to incidents related to the products or services provided to the entity that pose cyber security risk to the entity. To meet this requirement, the vendor may have aligned with numerous cyber security frameworks (see table 1 in attachment B).

Notification when Remote or Onsite Access is No Longer Needed or Should No Longer be Available to Vendor Representatives

Vendors should respond accordingly to personnel changes. A vendor should be able to tell the entity when a personnel change occurs that could impact whether or not remote access should still be available to vendor representatives. To meet this requirement, the vendor may have aligned with cyber security frameworks that control use of administrative privileges and/or control access based upon a need to know (see table 1 in attachment B).

Vulnerability Identification

Vendors are to notify an entity when a vulnerability related to a product or service is identified. In order to meet this obligation, a vendor needs to know when a vulnerability exists in their environment. To meet this requirement, the vendor may have aligned with cyber security frameworks that require continuous vulnerability assessment and mitigation to ensure that vulnerabilities are identified at the time of procurement and after procurement (see table 1 in attachment B).

Verification of Software Integrity and Authenticity of all Software and Patches Provided by the Vendor for Use in BES Systems

Vendors are to provide the capability to ensure the integrity and authenticity of all software and patches provided to an entity. In order to meet this obligation, a vendor may have aligned with cyber security frameworks that require application software security (see table 1 in attachment B).

Coordination of Controls for Vendor-Initiated Interactive Remote Access and System-to-System Remote Access with a Vendor

Vendors must coordinate with entities to control vendor-initiated interactive remote access and ensure system-to-system remote access with a vendor is appropriately managed. To meet this requirement, the vendor may have aligned with cyber security frameworks that require account monitoring and control (see table 1 in attachment B).

At a minimum, the vendor should align with the above 6 basic principles of cyber security. The entity may define additional criteria for any vendor, as described below.

As an entity performs a risk assessment and considers risk exposure of products or services to be procured in its environment, additional cyber security controls may be necessary to protect the entity's operating environment. An entity may consider obtaining and evaluating additional information regarding the vendor's capabilities with respect to the following security areas.

Asset, Change, and Configuration Management

Inventory of Authorized and Unauthorized Devices

- Physical devices and systems within the organization are inventoried
- Software platforms and applications within the organization are inventoried
- Organizational communication and data flows are mapped
- External information systems are catalogued

Change Control and Configuration Management Considerations

- Uses a recognized framework for its information technology processes (e.g., ITIL)
- Includes security in its system development life cycle
- Has a mature change-control process
- Maintains separate development and production environments
- Maintains separate environments for different customers
- Has mechanism for software integrity (e.g., PKI with encryption, digital signature)
- Product allows for hardening to minimize attack surface
- Processes to identify, discover, inventory, classify, and manage information assets (hardware and software)
- Processes to detect unauthorized changes to software and configuration parameters
- Able to identify whether hardware, software, or components are U.S. and/or internationally sourced

Governance

Establish and Implement Security Awareness Program

- Documented and implemented security policy and procedures
- All users are informed and trained on cybersecurity policies and procedures
- Third-party stakeholders understand roles and responsibilities and are accountable to same requirements
- Senior executives understand roles and responsibilities
- Physical and information security personnel understand roles and responsibilities
- Ability to provide ongoing support for software and hardware
- Personnel background checks
- Ability to retain data for events such as litigation holds, cyber security incidents
- Presence of trained, knowledgeable, and sufficient cyber security resources

- Supplier has certifications for manufacturing process (e.g., ISO)

Logging and Monitoring Considerations:

- Maintains a program to perform continuous logging, monitoring, and analysis of its systems to identify events of significance
- Has sufficient segregation of duties to ensure logging and monitoring are effective to detect anomalies

Information Protection Considerations

- Uses appropriate controls to manage data at rest (vendor or entity data)
- Ability to provide additional hardware for failures
- Encrypts credentials in transit, internal and externally
- Encrypts credentials at rest
- Uses strongest standard encryption algorithms (e.g., AES or SHA-2)
- Supplier physical access controls to hardware, software, and manufacturing centers
- Physical devices and systems within the organization are inventoried
- Supplier location of data centers (U.S./Canada-based vs international)

Attachment B – Cyber Security Framework Mapping

Entities use appropriate subject-matter experts to develop cyber security policy. Various security frameworks that entities may find useful for developing their cyber security policy are mapped in table 1 below. **Table 1 provides example mapping and is not an all-inclusive list.**

Notable cyber security frameworks and best practices include[7]:

- Center for Internet Security (CIS) Critical Controls
- NIST Cyber Security Framework
- PCI DSS
- HIPAA
- COBIT 5
- AICPA SOC 2 and SOC 3 Trust Services Criteria
- NATF Security Principles of Excellence
- NERC Reliability Standards

[7] Cyber security frameworks are frequently updated as cyber security risk evolves. Thus, Responsible Entities evaluate the latest version of these frameworks that best address risk in the impacted electric utility.

Table 1: Cyber Security Framework Mapping

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP Standards
1.2.1/1.2.2 Notification by the vendor of, and coordination of responses to, vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity	*Critical Security Control #19: Incident Response and Management*	*PR.IP-9* *PR.IP-10* *DE.AE-2* *DE.AE-4* *DE.AE-5* *DE.CM-1-7* *RS.RP-1* *RS.CO-1-5* *RS.AN-1-4* *RS.MI-1-2* *RS.IM-1-2* *RC.RP-1* *RC.IM-1-2* *RC.CO-1-3*	*12.10*	*164.308(a)(6): Security Incident Procedures - Response and Reporting R*	*APO13: Manage Security DSS05: Manage Security Services DSS02: Manage Service Requests and Incidents*	*CC2.3* *CC7.1-CC7.5* *CC9.2*	*CIP-008 R1* *CIP-008 R2* *CIP-008 R3*
1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives	*Critical Security Control #5: Controlled Use of Administrative Privileges* *Critical Security Control #14: Controlled Access Based on the Need to Know*	*PR.AC-4* *PR.AC-5* *PR.AT-2* *PR.DS-1* *PR.DS-2* *PR.IP-8* *PR.MA-2* *PR.PT-2* *PR.PT-3*	*1.3 - 1.4* *2.1* *4.3* *7.1 - 7.3* *8.1 - 8.3* *8.7*	*164.308(a)(1): Security Management Process - Information System Activity Review R* *164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R* *164.308(a)(4): Information Access Management - Access Authorization A* *164.310(b): Workstation Use - R* *164.310(c): Workstation Security - R* *164.312(a)(1): Access Control - Encryption and Decryption A* *164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A* *164.312(a)(1): Access Control - Automatic Logoff A* *164.312(d): Person or Entity Authentication - R* *164.312(e)(1): Transmission Security - Integrity Controls A* *164.312(e)(1): Transmission Security - Encryption A*	*APO13: Manage Security DSS05: Manage Security Services*	*CC5.2* *CC6.1-CC6.4* *CC9.2*	*CIP-004 R4* *CIP-004 R5* *CIP-005 R1* *CIP-005 R2* *CIP-007 R4* *CIP-007 R5* *CIP-011 R1*

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP Standards
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity	Critical Security Control #4: Continuous Vulnerability Assessment and Remediation	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 PR.IP-12 DE.CM-8 RS.MI-3	6.1 6.2 11.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	APO13: Manage Security DSS05: Manage Security Services	CC2.3 CC3.2 CC 6.1 CC 7.1-CC7.2 CC9.2	CIP-007 R2 CIP-010 R3
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System	Critical Security Control #18: Application Software Security	PR.DS-6 PR.DS-7 PR.IP-1 PR.IP-2 PR.IP-3 PR.MA-1	6.3 6.5 - 6.7		APO13: Manage Security DSS05: Manage Security Services	CC 6.8	CIP-010 R1
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)[8]	Critical Security Control #16: Account Monitoring and Control	PR.AC-1 PR.AC-3 PR.AC-4 PR.PT-3	7.1 - 7.3 8.7 - 8.8	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Access Authorization A 164.308(a)(4): Information Access Management - Access Establishment and Modification A 164.308(a)(5): Security Awareness and Training - Password Management A 164.312(a)(1): Access Control - Unique User Identification R 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	APO13: Manage Security DSS05: Manage Security Services	CC5.2 CC 6.1 -CC6.3 CC6.6 CC6.7	CIP-005 R1 CIP-005 R2 CIP-007 R4

[8] CIP-013 R1.2.6 Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s), is closely related to supply chain risk adjustments incorporated in version 6 of CIP 005 in Parts 2.4 and 2.5. Many best practice frameworks combine the responsibilities of vendors/suppliers and implementers to encourage more complete remediation of risk associated with interactive remote access. The mapping shown in the table reflects the coordination of vendor/supplier and implementer security controls.

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP Standards
Asset, Change, and Configuration Management	*Critical Security Control #1: Inventory of Authorized and Unauthorized Devices*	*DE.AE-1* *ID.AM-1* *ID.AM-3* *ID.AM-4* *PR.AC-2* *PR.DS-3*	*2.4*	*164.310(b): Workstation Use - R* *164.310(c): Workstation Security - R*	*APO13: Manage Security* *DSS05: Manage Security Services* *BAI09: Manage Assets*	*CC6.1* *CC6.8* *CC7.1* *CC8.1*	*CIP-002 R1* *CIP-002 R2* *CIP-010 R1*
Governance	*Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps*	*PR.AT-1* *PR.AT-2* *PR.AT-3* *PR.AT-4* *PR.AT-5* *PR.IP-11*	*12.6*	*164.308(a)(5): Security Awareness and Training - Security Reminders A* *164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A* *164.308(a)(5): Security Awareness and Training - Log-in Monitoring A* *164.308(a)(5): Security Awareness and Training - Password Management A*	*APO13: Manage Security* *DSS05: Manage Security Services*	*CC1.4, CC2.2,* *CC6.1* *CC9.2*	*CIP-003 R1* *CIP-004 R1* *CIP-004 R2* *CIP-004 R3*
Information Protection	*Critical Security Control #13: Data Protection*	*PR.DS-1* *PR.DS-2* *PR.DS-5* *PR.IP-4* *PR.IP-5* *PR.IP-6* *PR.IP-7* *PR.PT-2* *PR.PT-4*	*1.3 - 1.4* *4.3* *7.1 - 7.3* *8.7*	*164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R* *164.310(d)(1): Device and Media Controls - Accountability A* *164.312(a)(1): Access Control - Encryption and Decryption A* *164.312(e)(1): Transmission Security - Integrity Controls A* *164.312(e)(1): Transmission Security - Encryption A*	*APO13: Manage Security* *DSS05: Manage Security Services*	*CC6.1-CC6.5* *CC6.7* *CC8.1* *CC9.2* *C1.1-C1.2*	*CIP-011 R1*
Logging and Monitoring	*Critical Security Control #3: Secure Configurations for Hardware and Software*	*DE.AE-3* *DE.DP-1* *DE.DP-2* *DE.DP-3* *DE.DP-4* *DE.DP-5* *PR.PT-1*	*10.1 - 10.9*	*164.308(a)(1): Security Management Process - Information System Activity Review R* *164.308(a)(5): Security Awareness and Training - Log-in Monitoring A*	*APO13: Manage Security* *DSS05: Manage Security Services*	*CC7.1 - CC7.3*	*CIP-007 R4*