North American Generator Forum Cyber Security Supply Chain Management White Paper

September 18, 2018

North American Generator Forum
P.O. Box 462
Powell, OH 43065
(561) 904-3234
NAGF Contact: Wayne Sipperly - NAGF Executive Coordinator

MISSION

"The NAGF mission is to promote the safe, reliable operation of the generator segment of the bulk power system through generator owner and operator collaboration with others who have a vested interest in the reliable operation of the bulk power system."

It is the policy and practice of the Forum to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy and the related guidelines apply to all Forum Participants. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Each Forum Participant agrees to behave in a manner consistent with these guidelines and acknowledges and agrees that any Forum Participant who does not comply with these guidelines may be subject to disciplinary action, including, without limitation, expulsion from membership or participation in the Forum and such other relief as may be proper.

Contents

EXECUTIVE SUMMARY

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. (see Order No 829 at P 1)

The Cyber Security Supply Chain Risk Management Standard Drafting Team (SDT) drafted a new Reliability Standard, CIP-013-1, and proposed modifications to CIP-005 and CIP-010 to address these directives (the "Supply Chain Standards").

On August 10, 2017, the NERC Board of Trustees adopted the proposed Supply Chain Standards, and requested *"that each of the North American Transmission Forum and the North American Generation Forum (the "Forums") develop white papers to address best and leading practices in supply chain management, including procurement, specifications, vendor requirements and existing equipment management, that are shared across the membership of each Forum, and to the extent permissible under any applicable confidentiality requirements, distribute such white papers to industry,"* (see August 10, 2017 NERC BOT Meeting, agenda item 9.a P 1).

This document was created by the North American Generator Forum (NAGF) to facilitate industry work to improve reliability and resiliency. The Forum recommends that entities consult their own counsel and subject matter experts to determine those cyber security practices which best address their specific risks and needs.

PURPOSE

The North American Generator Forum (NAGF) developed this white paper to identify examples for generation entities to consider when developing and implementing a risk-based cyber security supply chain risk management plan. In addition, the NAGF provides this information for NERC to consider in the development of additional implementation guidance supporting CIP-013 R1.

GENERATOR SUPPLY CHAIN MANAGEMENT PRACTICES

Approach

The practices provided in this white paper represent a risk-based approach for generation entities to consider for developing supply chain cyber security risk management plans. The first step consists of an initial risk screen for assessing BES Cyber Systems or vendor services to determine if additional vendor supply chain evaluation is required. There are a number of attributes identified that Responsible Entities can consider for this pre-screen process. For systems or services that require vendor supply chain evaluation, attributes are identified for consideration to perform such an evaluation. The outcome of the initial risk screen and vendor supply chain analysis will determine the level of supply chain controls necessary for the remaining stages of the BES Cyber System life cycle: procure/acquire, deploy/implement, and operate/maintain. Various existing guidance, security frameworks, and best practices are available for entities to consider for developing their supply chain cyber security controls for the remaining stages of the BES Cyber System life cycle.

This risk-based approach for a supply chain cyber security management plan can be applied to all BES Cyber Systems/Assets including low impact assets and can be tailored to align with the organization's risk appetite and overall cyber security program.

INITIAL RISK TEST FOR BES CYBER ASSETS/SYSTEMS/SERVICES

An initial risk screening process can be performed by applying some or all of the following attributes to BES Cyber Systems or to vendor cyber support services for determining whether a vendor supply chain risk assessment is required. If, after considering these attributes, an entity determines the risk is minimal, the decision may be to document the results and not continue the vendor supply chain risk assessments for the asset/system/service.

- **CIP-002 Rating**

Determining the categorization level of an asset's BES Cyber Systems (high, medium, or low impact) is a risk assessment of the asset's potential impact to the BES. Entities may use this risk assessment, along with the other attributes in this section, to determine if an entity will complete vendor supply chain risk assessments for the asset, or, if the risk is determined to be minimal, document the results and conclude the assessment.

- **Asset Connectivity**

This attribute is intended to identify external connectivity to the BES Cyber Systems. If the BES Cyber Asset has any type of external electronic connectivity to a BES Cyber System, then it is a higher risk. Types of external connectivity can include, but are not limited to leased line, Internet connection, MPLS circuit, and dial-up.

- **Vendor Connectivity**

If there is external connectivity to the asset, are there technical and procedural processes in place to control (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access between cyber assets at the asset and the vendor? This includes the ability of entity staff to monitor established connections and to disconnect sessions as needed. The type of connectivity and the level of control the entity has will determine risk exposure.

- **Transient Cyber Assets (TCA) and Removable Media (RM)**

Allowing TCA and RM at the asset elevates the asset's security and compliance risk levels.

  - If TCA and RM are allowed at the asset, has a plan been implemented per *CIP-010-3 - Attachment 1*?

- **Support staff**

Support staff, and the level of experience of support staff, at an asset can have an impact on the risk rating of the asset. If, for example, there is no support staff located at a remote site where a BES Cyber Asset is located, the time required to resolve an issue may pose an elevated risk. A distinction should be made between entity employees and contracted employees, since contracted employees may be more likely to have a shorter tenure at an asset.

- **Security Awareness/Training**

The level and frequency of security awareness and training for entity or contract support staff can have an impact on the risk level of the asset.

- **Personnel Risk Assessment (PRA)**

The depth and frequency of PRAs performed on entity staff and contractors at an asset impact the risk level of the asset. Is a PRA performed on all new hires, and if so, is it renewed on a defined interval? This applies to entity employees as well as contractors, although the entity itself may not be performing the PRA for contractors.

VENDOR SUPPLY CHAIN RISK ASSESSMENT PROCESS

If the initial risk screen process of a BES Cyber System/Asset or vendor cyber support service determines that a vendor supply chain risk assessment is required, the following attributes can be considered as part of the vendor supply chain evaluation to determine the appropriate level of supply chain controls required for each of the remaining stages of the BES Cyber System life cycle.

Vendor Risk Attributes

- **Country of Origin**

The country where the vendor is located or headquartered should be considered. For example, if the vendor is located in the United States or a friendly foreign country (e.g. a Western European country) they are more likely to have supply chain security processes in place than a potentially hostile country.

- **History**

A company that is well established with a measurable length of time in business will be more likely to have mature business processes, including those applicable to supply chain security practices. A company that is less than a year old may pose a greater risk than a more established and mature company that has been doing business for a number of years.

- **Industry**

Evaluate the vendor to determine if it specializes in products for the electric utility industry or if it is a vendor like Microsoft or Cisco that markets software to very broad ranges of industries. This can be an important risk attribute in determining the level of specialized support available.

- **Core Business**

Is the vendor marketing a product that is part of its core business or has it recently acquired the product? A vendor that recently acquired a product or service may choose to discontinue the product or service or stop further development.

- **Type of Vendor**

What type of vendor is being evaluated (manufacturer, supplier, developer, integrator, or service provider)?

- **Component Supply**

Determine the risk posed by a vendor based on whether the vendor sources its physical or software components internally, domestically, or from a foreign country.

- **Personnel Changes**

Determine whether a vendor has a process to identify personnel with access to Responsible Entity systems or data and to take appropriate actions upon the change of status of said personnel.

- **Vendor Remote Access (CIP-013-1 R1.2.6)**

Does the vendor agree to adhere to the Responsible Entity's policies regarding controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access between cyber assets at the asset and the vendor?

- **Hardware Development Lifecycle (HDLC) or Software Development Lifecycle (SDLC) Process**

Vendors that have a documented HDLC, SDLC, or similar process would be viewed as a lower risk.

- **Security Vulnerability Testing Process**

Vendors that have a security program for identifying and remediating product security vulnerabilities would have a lower supply chain risk.

- **Notifications (CIP-013-1 R1.2.1, 1.2.3, 1.2.4)**

Determine if the vendor has a process to notify Responsible Entity of vendor-identified incidents related to the products or services provided that pose cyber security risk to the Responsible Entity. This can include cyber security incidents that may not directly impact the product or service itself, such as data breaches that disclose Responsible Entity data. Notifications should be included for the following attributes:

  - Personnel Changes,
  - HDLC/SLDC Process,
  - Security Vulnerability Testing Process, and
  - Patch Management

- **Coordination (CIP-013-1 R1.2.2)**

Determine if the vendor has a process to coordinate 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. Beyond the notification process, does the vendor have processes to provide notifications to Responsible Entities as soon as practicable, develop security updates and provide them to customers as soon as practicable, and identify compensating measures the Responsible Entity can implement?

Vendor Product/Service Attributes

- **Patch Management or Firmware Updates (CIP-013-1 R1.2.5)**

Vendors that have a security vulnerability testing process must provide:

  - Security updates in a timely manner
  - Adequate information to track patches
    - List of software/firmware
    - Versioning
    - Release dates
  - A means to ensure the authenticity and integrity of software and firmware it provides.

- **Logical Ports**

Does the vendor's product or software provide a mechanism to disable ports not specifically required? The ability to disable ports that are not required lowers the risk of security vulnerabilities.

- **User Accounts**

Does the vendor's product or service have a mechanism for user authentication and authorization? The ability to accept multi-factor authentication would lower the risk of security vulnerabilities.

- **Default Accounts**

Does the vendor provide an inventory or listing of all default or generic accounts included in its product or service and the means to disable or rename and change the password of identified accounts? If yes, the risk rating would be lower.

- **Password Complexity**

Does the vendor's product or service support password complexity and can it enforce password complexity and length requirements? If yes, the risk rating would be lower.

- **Malicious Code**

If the vendor's product or service can detect, deter, or prevent malicious code, or if it allows for the installation

of software to detect, deter, or prevent malicious code, the risk rating would be lower.

- **Event logging**

Determine if the vendor's product or service has the capability of logging the following types of events at a minimum:

  - Successful logins
  - Unsuccessful login and access attempts
  - Detected malicious code (if applicable)

- **Advanced Security Features**

Determine if the vendor's product or service includes security features that lower the risk of security vulnerabilities:

  - Application or service whitelisting
  - Storage Encryption
  - Communication Encryption
  - Multi-factor authentication

Information to assist with evaluating the attributes identified for the initial risk screening and optional vendor supply chain risk assessment can be obtained from sources such as the entity's own cyber security program, vendor questionnaire, independent third party certification, or existing industry certifications.

Periodic review of the risk-based cyber security supply chain risk management plan and assessment results should be performed in accordance with the overarching cyber security program.

INITIAL RISK SCREEN AND VENDOR SUPPLY CHAIN RISK ASSESSMENT DOCUMENTATION

A balanced scorecard or spreadsheet can be used to summarize and document the results of the initial risk screening and vendor supply chain risk assessment. Attachment A contains an example of a balanced scorecard approach summarizing the results of the assessments that a Responsible Entity can implement as part of its Cyber Security Supply Chain Risk Management Plan.

REMAINING STAGES OF THE BES CYBER SYSTEM LIFE CYCLE

There are a number of existing guidance, security frameworks, and best practices that entities may reference for developing cyber security supply chain controls associated with the stages of the BES Cyber System lifecycle:

- NIST Cyber Security Framework – Special Publication 800-161
- Cybersecurity Procurement Language for Energy Delivery Systems (CPLEDS)
- NATF Supply Chain Cyber Security Risk Management Guidance White Paper and Implementation Guidance (CIP-005-6 R2.4/2.5, CIP-010-3 R1.6, & CIP-013-1)
- NEMA Guideline Document CPSP 1-2015 - Supply Chain Best Practices
- EEI Principles and Resources for Managing Supply Chain Cybersecurity Risk
- NERC CIP-013-1 Cyber Security Supply Chain Technical Guidance and Examples

ACKNOWLEDGMENTS

The NAGF would like to recognize the following members for their contributions to this white paper:

James Fletcher

Scott Raymond

Andy Schiefelbein

Allen Schriver

Tina Wayand

ATTACHMENT A – SUPPLY CHAIN RISK ASSESSMENT SCORE CARD EXAMPLE

SUPPLY CHAIN RISK ASSESSMENT SCORECARD			
Assessment Date:		Initial Risk Assessment Rating:	Red/Yellow- Vendor Assessment req. Green - No Vendor Assessment req.
BES Cyber System:			
Supplier Name:		Vendor Supply Chain Assessment Rating:	Red/Yellow - Supply Chain controls needed. Green - minimal Supply Chain controls needed.
Reviewed By:			
Comments:			

INITIAL RISK ASSESSMENT				
Attribute	**Description**	**Risk Rating 1- Low, 3- Medium, 5- High**	**Attribute Weight**	**Weighted Risk (Risk Rating * Attribute Weight)**
CIP-002 Rating	Determining the categorization level of an assets BES Cyber Systems, (high, medium, or low impact), is a risk assessment of the assets potential impact to the BES. Entities may use this risk assessment, along with the other attributes in this section to determine if an entity will complete vendor supply chain risk assessments for the asset, or if the risk is determined to be minimal, document the results and conclude the assessment.	0	100%	0
Asset Connectivity	This attribute is intended to identify external connectivity to the BES Cyber Systems. If the BES Cyber Asset has any type of external electronic connectivity to a BES Cyber System, then it is a higher risk. Types of external connectivity can include, but are not limited to leased line, Internet connection, MPLS circuit, and dial-up.	0	100%	0
Vendor Connectivity	If there is external connectivity to the asset, are there technical and procedural processes in place to control (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access between cyber assets at the asset and the vendor. This includes the ability of entity staff to monitor established connections and to disconnect sessions as needed. The type of connectivity and the level of control the entity has will determine risk exposure.	0	100%	0
Transient Cyber Assets (TCA) and Removable Media (RM)	Allowing TCA and RM at the asset elevates the asset's security and compliance risk levels. • If TCA and RM are allowed at the asset, has a plan been implemented per CIP-010-3 - Attachment 1?	0	75%	0
Support Staff	Support staff, and the level of experience of support staff, at an asset can have an impact on the risk rating of the asset. If, for example, there is no support staff located at a remote site where a BES Cyber Asset is located, the time required to resolve an issue may pose an elevated risk. A distinction should be made between entity employees and contracted employees, since contracted employees may be more likely to have a shorter tenure at an asset.	0	25%	0
Security Awareness/Training	The level and frequency of security awareness and training for entity or contract support staff can have an impact on the risk level of the asset.	0	75%	0
Personnel Risk Assessment (PRA)	The depth and frequency of PRAs performed on entity staff and contractors at an asset impact the risk level of the asset. Is a PRA performed on all new hires, and if so is it renewed on a defined interval? This applies to entity employees as well as contractors, although the entity itself may not be performing the PRA for contractors.	0	50%	0
INITIAL RISK ASSESSMENT SCORE				**0**

VENDOR SUPPLY CHAIN ASSESSMENT				
VENDOR RISK ASSESSMENT				
Attribute	**Description**	**Risk Rating 1- Low, 3- Medium, 5- High**	**Attribute Weight**	**Weighted Risk (Risk Rating * Attribute Weight)**
Country of Origin	The country where the vendor is located or headquartered should be considered. For example, if the vendor is located in the United States or a friendly foreign country (e.g. a Western European country) they are more likely to have supply chain security processes in place than a potentially hostile country (e.g. North Korea, Syria, Russia, or China).	0	100%	0
History	A company that is well established with a measurable length of time in business will be more likely to have mature business processes, including those applicable to supply chain security practices. A company that is less than a year old may pose a greater risk than a more established and mature company that has been doing business for a number of years.	0	25%	0
Industry	Evaluate the vendor to determine if it specializes in products for the electric utility industry or if it is a vendor like Microsoft or Cisco that markets software to very broad ranges of industries. This can be an important risk attribute in determining the level of specialized support available.	0	25%	0
Core Business	Is the vendor marketing a product that is part of its core business or has it recently acquired the product? A vendor that recently acquired a product or service may choose to discontinue the product or service or stop further development.	0	50%	0
Type of Vendor	What type of vendor is being evaluated (manufacturer, supplier, developer, integrator, or service provider)?	0	50%	0
Component Supply	Determine the risk posed by a vendor based on whether the vendor sources its physical or software components internally, domestically, or from a foreign country.	0	25%	0
Personnel Changes	Determine whether a vendor has a process to identify personnel with access to Responsible Entity systems or data and to take appropriate actions upon the change of status of said personnel.	0	75%	0
Vendor Remote Access (CIP-013-1 R1.2.6)	Does the vendor agree to adhere to the Responsible Entity's policies regarding controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access between cyber assets at the asset and the vendor?	0	100%	0
HDLC or SDLC Process	Vendors that have a documented Hardware Development Lifecycle (HDLC), Software Development Life Cycle (SDLC) or similar process would be viewed as a lower risk.	0	75%	0
Security Vulnerability Testing Process	Vendors that have a security program for identifying and remediating product security vulnerabilities would have a lower supply chain risk.	0	100%	0
Notifications (CIP-013-1 R1.2.1, 1.2.3, 1.2.4)	Determine if the vendor has a process to notify Responsible Entity of vendor-identified incidents related to the products or services that pose cyber security risk to the Responsible Entity. This can include cyber security incidents that may not directly impact the product or service itself, such as data breaches that disclose Responsible Entity data. Notifications should be included for the following attributes: • Personnel Changes, • HDLC/SLDC Process, • Security Vulnerability Testing Process, and • Patch Management	0	100%	0
Coordination (CIP-013-1 R1.2.2)	Determine if the vendor has a process to coordinate 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. Beyond the notification process, does the vendor have processes to provide notifications to Responsible Entities as soon as practicable, develop security updates and provide them to customers as soon as practicable, and identify compensating measures the Responsible Entity can implement?	0	100%	0
VENDOR RISK ASSESSMENT SCORE:				**0**

VENDOR PRODUCT/SERVICE ASSESSMENT				
Attribute	**Description**	**Risk Rating 1- Low, 3- Medium, 5- High**	**Attribute Weight**	**Weighted Risk (Risk Rating * Attribute Weight)**
Patch Management or Firmware Updates (CIP-013-1 R1.2.5)	Vendors that have a security vulnerability testing process provide: • Security updates in a timely manner • Adequate information to track patches - List of software/firmware - Versioning - Release dates • A means to ensure the authenticity and integrity of software and firmware it provides.	0	75%	0
Logical Ports	Does the vendor's product or software provide a mechanism to disable ports not specifically required? The ability to disable ports that are not required lowers the risk of security vulnerabilities.	0	50%	0
User Accounts	Does the vendor's product or service have a mechanism for user authentication and authorization? The ability to accept multi-factor authentication would lower the risk of security vulnerabilities.	0	100%	0
Default Accounts	Does the vendor provide an inventory or listing of all default or generic accounts included in its product or service and the means to disable or rename and change the password of identified accounts? If yes, the risk rating would be lower.	0	75%	0
Password Complexity	Does the vendor's product or service support password complexity and can it enforce password complexity and length requirements? If yes, the risk rating would be lower.	0	75%	0
Malicious Code	If the vendor's product or service can detect, deter, or prevent malicious code, or if it allows for the installation of software to detect, deter, or prevent malicious code, the risk rating would be lower.	0	100%	0
Event Logging	Determine if the vendor's product or service has the capability of logging the following types of events at a minimum: • Successful logins • Unsuccessful login and access attempts • Detected malicious code (if applicable)	0	50%	0
Advanced Security Features	Determine if the vendor's product or service includes security features that lower the risk of security vulnerabilities: • Application or service whitelisting • Storage Encryption • Communication Encryption • Multi-factor authentication	0	50%	0
VENDOR PRODUCT/SERVICE ASSESSMENT SCORE:				**0**

VENDOR SUPPLY CHAIN ASSESSMENT SCORE:	**0**