CIP-013 Vendor Questionnaire

|  |  |
| --- | --- |
| Vendor Name:  |  |
| Date: |  |

CORE is a North American Electric Reliability Organization[[1]](#footnote-1) (NERC) Registered Entity and bound to the NERC Critical Infrastructure Protection (CIP) standards[[2]](#footnote-2). In support of Supply Chain Risk Management (the CIP-013-2[[3]](#footnote-3) standard), CORE is seeking information from suppliers of vendor products and services related to assessment of cyber security risk(s) to our Bulk Electric System Cyber Assets[[4]](#footnote-4).

**Purpose:** Completion of this questionnaire provides CORE an understanding of cyber security controls and processes the supplier/vendor has currently implemented or is able to include in the terms and conditions of any contract in agreement to provide hardware, software or services to CORE as required by the North American Reliability Corporation (NERC) regulatory requirements pertaining to the Critical Infrastructure Protection (CIP) standard CIP-013-2.

Per the language of Requirement 1.2 of CIP-013-2, CORE is asking all suppliers to provide information necessary for this assessment process. Responses to the following questions are required.

1. NERC requires notification to CORE concerning cyber security incidents related to the products or services provided to CORE. What is your method for providing these notices (e.g. email, website, RSS)?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

1. NERC requires coordination of responses to vendor-identified incidents that pose cyber security risk related to the products or services provided to CORE. What is your method for identifying cyber security incidents? What is your method for coordination of relevant response actions?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

1. NERC requires CORE to revoke access within 24 hours when remote or onsite access is no longer needed by your personnel to CORE systems or facilities. What is your method for providing these notices (e.g. email, phone)?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

1. NERC requires notification to CORE of known cybersecurity vulnerabilities related to the products or services provided to CORE. What is your method for providing these notices (e.g. email, website, RSS)?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

1. NERC requires verification and notification of software integrity (e.g. cryptographic hash or checksum[[5]](#footnote-5)) and authenticity of all software and patches provided to CORE. What is your method for providing these verifications (e.g. email, website)?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

1. What methods for Interactive Remote Access4 do you support?

Vendor Response (if a process is not currently in place, please indicate if there is an ability to implement this process in order to provide products or services to CORE):

CORE is asking all suppliers to voluntarily provide the following additional information that will factor into this assessment process:

1. In relation to change control and configuration management considerations, which of the following controls has your organization implemented?

[ ]  Use 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., hashing, digital signature)

[ ]  Product allows for hardening to minimize attack surface

[ ]  Processes to detect unauthorized changes to source code, compiled software and/or configuration parameters

[ ]  Able to identify whether hardware, software, or components are U.S. and/or internationally sourced

1. In relation to security governance, which of the following controls has your organization implemented?

[ ]  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 are responsible and accountable for security

[ ]  Physical and information security personnel have clear organizational roles

[ ]  Ability to provide ongoing support for software and hardware

[ ]  Personnel background checks are performed on key personnel

[ ]  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)

1. In relation to security logging and monitoring considerations, which of the following controls has your organization implemented?

[ ]  Maintains a program to perform continuous security logging, monitoring, and analysis of its systems to identify events of significance

[ ]  Has sufficient human and technical resources to ensure logging and monitoring to effectively detect security anomalies

1. In relation to information protection considerations, which of the following controls has your organization implemented?

[ ]  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)

CORE will include the relevant and applicable CIP-013 regulatory requirements as Terms and Conditions in contracts in order to maintain compliance with this federal regulation.

1. <https://www.nerc.com/Pages/default.aspx> [↑](#footnote-ref-1)
2. <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx> [↑](#footnote-ref-2)
3. <https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-2&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&jurisdiction=null> [↑](#footnote-ref-3)
4. <https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf> [↑](#footnote-ref-4)
5. <http://www.isaca.org/Knowledge-Center/Lists/ISACA%20Glossary%20Terms/DispForm.aspx?ID=1091> [↑](#footnote-ref-5)