NERC Continues to Provide Transition Guidance for CIP Standards

FERC may not approve CIP V5-6 before the end of 2015

FERC’s recently released Notice of Proposed Rulemaking (NOPR) for CIP V5-6 was a key topic of discussion at NERC’s August Board of Trustees meeting with much tension around the current April 2016 enforcement date. New issues introduced by the NOPR create uncertainty for the industry. FERC is currently receiving comments on the proposed changes and is unlikely to take final action before the end of 2015, leaving many questions as to the final content of all the CIP standards.

NERC is also revisiting its guidance for certain portions of the proposed standards related to Control Centers and which Control Centers are to be protected to what level (High, Medium or Low Impact) to support the industry in its efforts to be ready for the April 2016 enforcement date.

Standards Proposed for Approval by FERC

The following standards have been submitted to by NERC to FERC for approval.

- CIP-003-6 – Cyber Security – Security Management Controls
- CIP-004-6 – Cyber Security – Personnel and Training
- CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems (subject to further changes)
- CIP-007-6 – Cyber Security – Systems Security Management
- CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-2 – Cyber Security – Information Protection

Approval Background

On November 22, 2013, the Federal Energy Regulatory Commission (FERC) issued Order No. 791 approving NERC’s version 5 CIP standards and implementation. The Order authorized the direct transition to the new CIP standards allowing utilities to skip the interim version of the standards known as CIP Version 4.

On February 12, 2015 the NERC Board of Directors approved all proposed industry approved changes to the Critical Infrastructure Protection (CIP) Reliability Standards that are necessary to respond to the directives issued in the FERC final November 2013 approval order. On February 13, 2015 NERC filed the petition containing the necessary revisions with FERC. The NERC petition presented the technical basis and purpose of the proposed Reliability Standards along with a summary of the development history.

For more information, please contact: Scott Tezak, National Security Practice Leader- Technology at stezak@trcsolutions.com or 978.656.3675.
The proposed CIP standards provide for new cyber security controls and require that more utility control systems be protected. Due to the complexity of the changes, NERC had initiated a CIP Transition Program and conducted compliance pilot studies to help utilities prepare the new CIP standards and reduce the number of potential violations.

Registered entities should be well underway with their implementation plans in order to be compliant by the earliest of the effective dates for the new standards commencing April 2016.

**July 2015 FERC Notice of Proposed Rulemaking (NOPR)**

In a NOPR issued on July 16, 2015 FERC proposed to adopt the changes put forward by NERC in response to FERC’s prior directives. However FERC identified several concerns and requested a new initiative regarding supply chain issues related to the acquisition of Operating Technology equipment to address risks to communication networks and related bulk electric system assets. The proposal would call for the development of new standards for supply chain management security controls to protect the electric system from introduction of new security vulnerabilities and malware threats.

FERC is seeking comment on the proposal related to what would constitute a reasonable time frame to address supply chain management, along with the features of such a standard. The goal is to create a forward-looking, objective-driven standard that encompasses activities in the system development life cycle from research and development, design and manufacturing to acquisition, delivery, integration, operations, retirement and eventual disposal of the equipment and services.

The controls should accommodate differences among companies with regard to procurement, vendor relations, system requirements, information technology implementation and privileged commercial or financial information, using the National Institutes of Standards and Technology (NIST SP 800-161) as guidance. A standard pertaining to supply chain management security would:

- Address only the obligations of entities registered under FERC reliability rules;
- Be forward-looking and not require abrogation or renegotiation of contracts;
- Set goals about what to do while allowing flexibility for how an entity achieves those goals;
- Allow for exceptions given the diversity of acquisition processes; and
- Be specific enough so that compliance obligations are clear and enforceable.

FERC also proposes that NERC will develop certain modifications to Reliability Standard CIP-006-6, including changes to require protection for communication network components and data communicated between all bulk electric system Control Centers. In addition, FERC is seeking comments on the adequacy of the security controls incorporated in the current CIP Reliability Standards regarding remote access for electric system control communications. FERC stated that while the technical controls in proposed Reliability Standard CIP-006-6 are generally consistent with the type of controls cited in its Order No. 791, FERC is concerned that a reliability gap
exists because the applicability of the proposed standard is limited to BES Cyber Assets within the same Electronic Security Perimeter. This would leave the systems outside the Electronic Security Perimeter vulnerable.

**Key Definitions**

The following final definitions to be used in the revised standards highlight the types of systems and processes which registered entities must adapt to:

**BES Cyber Asset (BCA):** A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

**Low Impact BES Cyber System Electronic Access Point (LEAP):** A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

**Low Impact External Routable Connectivity (LERC):** Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).^1^

**Protected Cyber Assets (PCA):** One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

**Removable Media:** Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

---

^1^ FERC expressed concerns with the LERC definition in Sections 68-70 on pages 43 and 44 of the NOPR and seeks comment on the words “direct” and “Layer 7 application layer break.”

For more information, please contact: **Scott Tezak, National Security Practice Leader- Technology** at stezak@trcsolutions.com or 978.656.3675.


**Transient Cyber Asset:** A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

**Anticipated Effective Dates**

Order No. 791 covering the approved V5 standards still remains effective April 1, 2016. Depending on the timing and type of FERC action following the July 16 NOPR, the CIP V6 standards enforcement dates are projected to occur between April 1, 2016 and September 1, 2018.

**Specific Transition Guidance is Available**

At the request of industry, NERC has created a number of guidance documents and has published the results of the compliance trials for the new CIP standards. The materials are available on a special “Initiatives” project page for CIP Implementation. Utilities should review this material in detail as they prepare plans for the transition to the new CIP standards.

While many of the implementation issues discovered in the pilot study period were relatively straightforward, some were particularly challenging and required significant time and effort to address sufficiently. It is important to review this report and other guidance found on the NERC CIP Transition page to support your company’s compliance success.

**Next Steps**

Utilities should continue the process of adapting their compliance programs to these new standards in advance of the anticipated effective dates.

**Resources**

- FERC Order 791
- FERC Order 791-A
- NERC Petition to FERC with Revised CIP Standards
- NERC CIP Standards Development Project
- NERC CIP Transition Program Initiative Page
- NERC CIP Transition Implementation Guidance
About Us

TRC’s Technology Engineering Services Practice has an in-depth understanding of power generation, transmission engineering, operational technology and the latest security, building safety, and security management systems on the market. We also provide a suite of communication engineering services for all utility networks. We are well versed in the regulatory documents driving infrastructure protection. Our 40 security staff nationwide know what it takes to secure our Nation’s infrastructure based on 30 years of experience executing design contracts, guiding clients through mitigation and implementation projects, and providing testing and commissioning services. We work with clients on forward-thinking and forward-leaning initiatives related to the physical and cyber protection and “hardening” of critical infrastructure. Our team includes former utility directors and program managers with direct industry experiences with the NERC standards and managing risk-based programs. We have the expertise needed to assess, design, oversee, implement and test the security technology for an effective cyber and physical security program.

TRC’s Power Delivery Engineers provide full service transmission, substation and relay engineering, consulting and construction management for utilities, municipalities and industry. Comprised of over 1,000 personnel, many of whom are experienced utility engineers, our project teams know how to plan, design, and install systems and facilities that meet a client’s compliance, financial, technical, and scheduling goals. Our NERC compliance experts support projects from studies and ratings through maintenance and testing.

This regulatory update is a service to our utility clients, helping keep them informed of issues that impact their reliability risk and business goals.

September 1, 2015

For more information, please contact: Scott Tezak, National Security Practice Leader- Technology at stezak@trcsolutions.com or 978.656.3675.