NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards Transition Guidance

To: Regional Entities and Responsible Entities

From: NERC Compliance Operations and Critical Infrastructure Departments

Date: April 11, 2013

Background and Identification of Critical Assets or Bulk Electric System ("BES") Cyber Systems

The Critical Infrastructure Protection ("CIP") Version 3 Reliability Standards ("CIP Version 3") are currently mandatory and enforceable for Responsible Entities. The Federal Energy Regulatory Commission ("FERC") approved Version 4 of the CIP Reliability Standards ("CIP Version 4")[1] on April 19, 2012, in FERC Order No. 761.[2] The North American Electric Reliability Corporation ("NERC") filed the CIP Version 5 Reliability Standards ("CIP Version 5") with FERC on January 31, 2013, which are pending FERC approval.

In each of the CIP Versions 3 through 5, CIP-002 includes a requirement that an entity identify those assets that are subject to compliance with the remainder of the family of CIP Reliability Standards. CIP-002-3 requires an entity to have a risk-based assessment methodology ("RBAM") to determine its Critical Assets. CIP-002-4 requires an entity to use a bright-line criteria methodology, as set forth in Attachment 1 of CIP-002-4, to define Critical Assets. CIP-002-5 requires an entity to use impact rating criteria in Attachment 1 of the standard to classify the level of impact of a BES Cyber System and to determine the corresponding compliance obligations. If CIP Version 5 and the corresponding implementation plan are approved by FERC as filed, prior to CIP Version 4 becoming enforceable, language in the implementation plan would go into effect. This would allow an entity to continue compliance with CIP Version 3 until CIP Version 5 becomes mandatory and enforceable. Under this scenario, CIP Version 4 would never be mandatory and enforceable.

[1] In addition, FERC approved the "Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4" and the "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities."

[2] http://www.nerc.com/files/OrderApprovingV4CIPStds-Order761_20120419.pdf. FERC Order No. 761 became effective on June 25, 2012. Order No. 761 was published in the Federal Register on April 25, 2012, with an effective date 60 days after publication. Therefore, the effective date of Order No. 761 is June 25, 2012. CIP Version 4's implementation plan provides for CIP Version 4 to become enforceable on April 1, 2014.

In the event that CIP Version 5's implementation plan is not approved by FERC or is not approved before April 1, 2014 (CIP Version 4's implementation date), then Responsible Entities must be compliant with CIP Version 4 by April 1, 2014.[3] However, compliance is subject to the provisions of the CIP Version 4 implementation plan for newly identified assets and newly registered entities that were approved by FERC in Order No. 761.[4] In its CIP Version 5 filing, NERC stated that it will work with industry to address transition issues.

Applicable Methodologies and Possible Outcomes

This section is intended to provide guidance to Regional Entities and Responsible Entities regarding the transition from CIP Version 3 to CIP Version 4 while CIP Version 5 is pending at FERC (referred to herein as the "Transition Period"). Once Version 5 is approved by FERC, NERC will provide additional transition guidance.

Responsible Entities must choose **one** of the following methodology approaches for CIP-002 during the Transition Period:[5]

- **Approach 1:** Maintain a valid CIP Version 3 RBAM with a complete risk-based discussion and justification for all Critical Asset selections made. This risk-based discussion may reach conclusions supported by the CIP Version 4 bright-line criteria, but the risk-based discussion is essential to meeting the RBAM requirements. Guidance developed by the CIP Version 4 standards drafting team may be useful in developing these risk-based discussions.[6]

- **Approach 2:** Adopt the CIP Version 4 bright-line criteria in its entirety, with the exception of criterion 1.4 Blackstart Resources and criterion 1.5 Cranking Paths. Control centers associated with Blackstart Resources (Criterion 1.15) and Cranking Paths (Criterion 1.16) shall continue to be deemed critical regardless of the aforementioned exclusion. Entities choosing this approach will not be required to maintain an RBAM document or a risk-based discussion justifying their conclusion. Additional effective and enforceable date clarifications are as follows:

    - CIP Version 4 assets identified between April 19, 2012 and June 25, 2012: The enforcement date is the later of Milestone Category 1 in Table 2 of the CIP Version 3

[3] The dates for compliance are enumerated in "Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4" and "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities."

[4] NERC notes that an incorrect version of the CIP Version 4 implementation plan for newly identified assets and newly registered entities was posted on the NERC website. The correct version is now posted and is available at: http://www.nerc.com/fileUploads/File/CIP_V4_Implementation_Plan_Newly_ID_Registered_Assets.pdf.

[5] If CIP Version 5 and the corresponding implementation plan are approved by FERC as filed, language in the implementation plan would go into effect that would allow an entity to continue compliance with CIP Version 3 until CIP Version 5 becomes mandatory and enforceable. As a result, CIP Version 4 would never be mandatory and enforceable. In that event, Responsible Entities that chose Approach 2 would be deemed to have a valid CIP Version 3 RBAM.

[6] *See* CIP-002-4 Cyber Security – Critical Cyber Asset Identification.

"Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities" *or* April 1, 2014.

- CIP Version 4 in-service assets meeting the bright-line criteria as of June 25, 2012: The date the standard becomes enforceable is April 1, 2014.
- CIP Version 4 assets identified by a third-party notification: The enforceable date for compliance will be determined by the CIP Version 4 "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities" with the start date being the date that notification is sent by the third-party.

Responsible Entities must identify which approach they have selected as part of their response to a pre-Compliance Audit Survey, a pre-Spot Check data request, or as otherwise requested pursuant to the Compliance Monitoring and Enforcement Program. In assessing the potential impacts of moving to CIP Version 4 (as stated in Approach 2) for all assets in service as of June 25, 2012, NERC offers the following additional compliance and enforcement guidance:

- **Assets that are newly subject to CIP Version 4:** Responsible Entities that will have new assets identified under the CIP Version 4 bright-line criteria between June 25, 2012 and April 1, 2014 should follow the FERC-approved implementation plan for CIP Version 4. This means that assets that met the CIP-002-4 Attachment 1 bright-line criteria as of the effective date of Order No. 761, which is June 25, 2012, must be compliant with all aspects of CIP Version 4 on April 1, 2014.[7]

- **Assets that are candidates for potential removal:** Pursuant to CIP-002-3, Responsible Entities may adjust their RBAM at any time, but must review it annually. NERC has provided industry the option to choose to adopt CIP Version 4 bright-line criteria as described in Approach 2, as their CIP Version 3 RBAM at any time prior to April 1, 2014. In these limited circumstances, entities may remove assets no longer deemed to be in scope of the bright-line criteria, as applicable. Responsible Entities should contact their Reliability Coordinator, Transmission Planner or Planning Authority to verify whether the asset can be removed from their Critical Asset list.[8]

- **Assets that meet both CIP Version 3 and CIP Version 4 criteria:** Current Critical Assets identified as critical under CIP Version 3 that will also be identified as critical under CIP Version 4 will be the primary focus of NERC and Regional Entity CIP Compliance Audits and related compliance monitoring activities with respect to Responsible Entities during the Transition Period.

[7] The dates for compliance are enumerated in "Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4" and "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities."

[8] *See also* Section 501.1.3.5 of the NERC Rules of Procedure, Organization Registration and Certification.

Compliance Monitoring and Enforcement Guidance

During the Transition Period, NERC's guidance is that NERC and Regional Entity CIP Compliance Audits will primarily focus on Responsible Entities' Critical Assets (under CIP-002-4 Attachment 1). In addition, NERC's guidance is that assets that would have been considered "critical" in CIP Version 4 but are "Low" impact Cyber Systems in CIP Version 5, such as Blackstart Resources and Cranking Path, will not be considered in the scope of Compliance Audits during the Transition Period. In circumstances where entities elect Approach 1 above, only assets that would be deemed critical under CIP Version 4 will be included for compliance monitoring actions. As previously described, the entity would remain subject to compliance under its Version 3 RBAM, and assets newly identified under CIP Version 4 would not be assessed for compliance until after April 1, 2014.

Additionally, Attachment 1 to CIP-002-4 recognizes that Reliability Coordinators, Transmission Planners, Planning Coordinators and Planning Authorities may identify Facilities that are necessary to avoid BES Adverse Reliability Impacts or that are deemed critical to the derivation of Interconnection Reliability Operating Limits ("IROLs") and their associated contingencies, which are then identified as Critical Assets or BES Cyber Systems of an affected Responsible Entity.[9] NERC's guidance to Regional Entities is that the Regional Entities will encourage this review, identification and communication of such Facilities. NERC grants Regional Entities the ability to manage disputes between Responsible Entities in resolving issues associated with Criterion 1.3, 1.8, 1.9 or 1.10 (see below) which may affect an entity's identified critical assets. For example, the following CIP Version 4 criteria could require more Facilities to be designated as Critical Assets if the CIP Version 4 criteria are adopted as the CIP Version 3 RBAM or limit the assets that may be delisted under Approach 2:

- CIP Version 4 – Criteria 1.3: Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.
- CIP Version 4 – Criteria 1.8: Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of IROLs and their associated contingencies.
- CIP Version 4 – Criteria 1.9: Flexible AC Transmission Systems, at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of IROLs and their associated contingencies.
- CIP Version 4 – Criteria 1.10: Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

[9] Under these circumstances, the affected Responsible Entity shall reference the CIP Version 4 "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities."

Compliance Enforcement Authorities (CEAs) are advised that Compliance Application Notice (CAN)-0012 *Completion of Periodic Activity Requirements during Implementation Plan*, does not apply to this implementation plan and will not be accepted as a reason for Responsible Entity noncompliance by the enforcement date of CIP-002-4.[10] CAN-0012 provides:

> In the event that a standard that is subject to an implementation plan, which contains a requirement of a periodic activity, the implementation plan may establish when the first occurrence of the periodic activity was to be completed. In that case, CEAs are to verify that the registered entity has completed the activity at least once before the enforceable date of the standard. However, in the event that the standard or implementation plan is silent with regard to completing a periodic activity, CEAs are to verify that the registered entity has performed the periodic activity within the standard's timeframe after the enforceable date.

The CIP Version 4 implementation plan is silent on whether the annual review (the periodic activity) must be conducted prior to the enforceable date of April 1, 2014. Under the guidance of CAN-0012, a registered entity would have up to an annual period (as defined by CAN-0010, *Implementation of Annual in Reliability Standards Requirements).* As CAN-0012 will not be accepted as a reason for a Responsible Entity's noncompliance by the enforcement date of CIP-002-4, a Responsible Entity must have completed its annual review as required by the standard prior to the enforceable date (April 1, 2014).

Instances of potential noncompliance that have been identified in compliance monitoring activities prior to this guidance may be closed with no further action, processed using the Find, Fix, Track and Report tool, if appropriate, or processed in accordance with the NERC Rules of Procedure.

NERC understands the need for flexibility during the Transition Period and stands committed to work with industry to address any potential transition issues. For more information or assistance relating to transition compliance issues please contact:

Matt Blizard
Director of Critical Infrastructure Protection
matt.blizard@nerc.net

Earl W. Shockley
Senior Director of Compliance Operations
earl.shockley@nerc.net

[10] http://www.nerc.com/files/CAN-0012%20Completion%20of%20Periodic%20Activity%20Requirements%20During%20Implementation%20Plan%20(Revised).pdf.