



NEW BRUNSWICK
ENERGY & UTILITIES BOARD
COMMISSION DE L'ÉNERGIE ET DES SERVICES PUBLICS
NOUVEAU-BRUNSWICK

Compliance Guidance Statement

NBEUB CGS 2015-002

Cyber Security Reliability Standards CIP V5 Transition Guidance

Effective September 1, 2015

1. Introduction

This document outlines the New Brunswick Energy and Utilities Board (“NBEUB”) proposed approach to compliance and enforcement activities as entities transition to the new and modified Critical Infrastructure Protection (“CIP”) Reliability Standards, referred to as the CIP Version 5 Reliability Standards (the “CIP V5 Standards”), approved by the NBEUB in Matter 246.¹ This Compliance Guidance Statement is based on the North American Electrical Reliability Corporation (“NERC”) CIP Version 5 transition guidelines which have been adapted for use in New Brunswick. The CIP V5 Standards represent an improvement over the currently effective CIP Reliability Standards, referred to as the CIP V3 Reliability Standards (the “CIP V3 Standards”), by adopting new cyber security controls and extending the scope of the systems protected by the CIP V3 Standards.² To support an efficient and effective transition to the CIP V5 Standards, the NBEUB will take a flexible compliance monitoring and enforcement approach for the CIP Reliability Standards prior to the effective date of the CIP V5 Standards (the “Transition Period”) and allow entities subject to the CIP V5 Standards (“Responsible Entities”) to implement the CIP V5 Standards, in whole or in part, during the Transition Period.³

¹ Version 5 Critical Infrastructure Protection Reliability Standards. The CIP V5 Standards consist of Reliability Standards CIP-002-5.1, CIP-003-5, CIP-004-5.1, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1.

² The CIP V3 Standards consist of currently effective Reliability Standards CIP-002-3, CIP-003-3, CIP-004-3a, CIP-005-3a, CIP-006-3c, CIP-007-3a, CIP-008-3, and CIP-009-3.

³ This document applies to the Compliance Body and Responsible Entities.

Responsible Entities are allowed to transition from compliance with the CIP V3 Standards directly to compliance with the CIP V5 Standards. For Responsible Entities, the requirements in the CIP V5 Standards will become effective on July 1, 2016. As explained in greater detail below, during the Transition Period, Responsible Entities may transition to implementing requirements in the CIP V5 Standards. The NBEUB will view a Responsible Entity's implementation of the requirements in the CIP V5 Standards as a proxy for compliance with requirements in the CIP V3 Standards.

2. Compliance and Enforcement Approach for the Transition Period

As a practical matter, the NBEUB understands that Responsible Entities cannot complete transition to the CIP V5 Standards in a single instance; rather, transition to full implementation will occur over a period of time as Responsible Entities develop the necessary procedures, software, facilities, or other relevant capabilities necessary for effective compliance with the CIP V5 Standards. To help ensure that they are fully compliant with the CIP V5 Standards upon the effective date, Responsible Entities may need or prefer to transition from compliance with the requirements of the CIP V3 Standards to implementation of the requirements of the CIP V5 Standards during the Transition Period. As such, there may be a period of time prior to the effective date of the CIP V5 Standards date when Responsible Entities begin to operate in accordance with the CIP V5 Standards while the CIP V3 Standards are still mandatory and enforceable.

The NBEUB thus recognizes the need for greater clarity and flexibility in its compliance and enforcement approach throughout this Transition Period to allow Responsible Entities to transition to the CIP V5 Standards in a manner and in a timeframe that best suits their needs and characteristics. As mentioned above, the NBEUB will therefore allow Responsible Entities to transition to the CIP V5 Standards, in whole or in part, during the Transition Period. In short, Responsible Entities may: (1) continue to comply with all of the CIP V3 Standards during the Transition period, or (2) begin transitioning to compliance with some or all of the CIP V5 Standards. The goal is to support Responsible Entities' implementation of the CIP V5 Standards as early as necessary to ensure that they may become fully compliant with the CIP V5 Standards by their effective date.

To support an efficient transition, a compatibility table (V3-V5 Compatibility Table) was developed which lists each of the requirements in the CIP V5 Standards and identifies whether the requirement is: (a) compatible or mostly compatible with a requirement in the CIP V3 Standards; or (b) a requirement new to the CIP V5 Standards that does not correlate to a CIP V3 requirement.⁴ A CIP V5 requirement is compatible with a CIP V3 requirement where the content and compliance expectation of the CIP V5 requirement is substantively similar to a corresponding CIP V3 requirement.

Prior to an audit, Spot Check or other compliance monitoring activity, the Responsible Entity shall notify the NBEUB and the Northeast Power Coordinating Council (NPCC), as described in Section 5 of this document, whether it has transitioned, or is in the process of transitioning, to implementing a particular CIP V5 Standard or requirement. If the Responsible Entity has notified the NBEUB and NPCC that it has transitioned, or is in the process of transitioning, to a CIP V5 requirement that is mostly compatible with a CIP V3 requirement, the NBEUB and NPCC compliance monitoring activities will focus on the Responsible Entity's implementation of the CIP V5 requirement, not the compatible CIP V3 requirement. If the Responsible Entity satisfies the obligations of the CIP V5 requirement, the NBEUB and NPCC will not also review the Responsible Entity's compliance with the compatible CIP V3 requirement. The

⁴ The V3-V5 Compatibility Table is available at <http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx>.

Responsible Entities' compliance with the CIP V5 requirement will be deemed as compliance with the compatible CIP V3 requirement.

For instance, Reliability Standard CIP-006-3c requires Responsible Entities to use a "6-walled perimeter" to provide for the physical security of Critical Cyber Assets (CIP-006-3c). The compatible CIP V5 Standard, CIP-006-5, however, does not require the "6-walled perimeter," relying on other access control and monitoring methods to protect BPS Cyber Systems. Where a Responsible Entity has transitioned to implementing CIP-006-5 during the Transition Period, the NBEUB and NPCC will focus on the Responsible Entity's implementation of the requirements of CIP-006-5, not whether the Responsible Entity has complied with CIP-006-3c and has a "6-walled perimeter." Similarly, during the Transition Period a Responsible Entity may begin implementing the malware protection requirements of CIP-007-5, which provide greater flexibility than the compatible CIP V3 Standard, CIP-007-3a. Reliability Standard CIP-007-5 allows entities to use network-based tools or whitelisting controls, whereas Reliability Standard CIP-007-3a requires strict application of device-based malware protection. Implementation of the more flexible approach provided in CIP-007-5 during the Transition Period will be deemed compliance with CIP-007-3a.

The NBEUB, however, must make certain that its flexible approach during the Transition Period does not create risks to the security and reliability of the Bulk-Power System. Accordingly, if a Responsible Entity notifies the NBEUB and NPCC that it has transitioned to a CIP V5 requirement but patently fails to meet the requirements of those standards and cannot demonstrate that it has taken reasonable steps towards implementation, the NBEUB's compliance and enforcement approach will be as follows: The NBEUB and NPCC will assess whether the Responsible Entity continues to comply with the compatible CIP V3 requirement (i.e., even if the Responsible Entity is not satisfying the CIP V5 requirement, the NBEUB and NPCC will assess whether the Responsible Entity is still meeting the core obligations of the CIP V3 requirement). If so, the Responsible Entity will have met its obligation to comply with the currently-effective CIP Reliability Standards (i.e., the CIP V3 Standards). If, however, the Responsible Entity does not satisfy a CIP V5 requirement and also does not comply with the compatible CIP V3 requirement, the Responsible Entity may be deemed non-compliant with the currently-effective CIP Reliability Standards and could be subject to an enforcement action in accordance with the New Brunswick Compliance Monitoring and Enforcement Program – Schedule A to the *Reliability Standards Regulation-Electricity Act* ("NB CMEP"). The goal is to ensure that that Responsible Entities continue to protect the security of their systems throughout the Transition Period, whether through continued compliance with the CIP V3 Standards or the implementation of the CIP V5 Standards.

Importantly, in assessing a Responsible Entity's implementation of a CIP V5 requirement during the Transition Period, the NBEUB will take a balanced approach, providing Responsible Entities latitude to mature under the CIP V5 Standards. The NBEUB understands that even for the CIP V3 requirements deemed compatible with CIP V5 requirements, the CIP V5 Standards contain new language and concepts and use a different approach for the identification of assets that Responsible Entities must protect under the CIP Reliability Standards. Accordingly, if a Responsible Entity meets the obligations of the CIP V5 requirements to which it has transitioned, even if certain elements of the compliance program can be improved, the NBEUB and NPCC will not proceed to review compliance with the compatible CIP V3 requirement.

For requirements in the CIP V5 Standards that are entirely new, as identified in the V3-V5 Compatibility Table, the NBEUB encourages entities to begin implementing those requirements during the Transition Period. The NBEUB and NPCC are available to discuss and review a Responsible Entity's approach to

implementing such requirements, although the compliance monitoring and enforcement activities will not focus on these new requirements.

Lastly, if a Responsible Entity has yet to transition to compliance with a CIP V5 requirement and notifies the NBEUB and NPCC that its compliance monitoring activities should focus on a CIP V3 requirement, the NBEUB and NPCC will continue to audit the Responsible Entity’s compliance with the CIP V3 requirement.

3. Asset Identification Options

A fundamental component of each version of the CIP Reliability Standards is the identification of cyber assets that Responsible Entities must protect under the CIP Reliability Standards. The CIP V3 Standards (CIP-002-3) require Responsible Entities to identify protected assets using a risk-based assessment methodology (“RBAM”). The CIP V5 Standards (CIP-002-5.1) also use bright-line criteria but, in addition, require Responsible Entities to categorize their systems into High, Medium, and Low Impact BPS Cyber Systems. Consistent with the principles discussed above, Responsible Entities may select from the following options for maintaining compliance with the effective CIP Reliability Standards during the Transition Period:

Options provided to the Industry in Support of the Transition to Version 5	
Continue to comply by maintaining a valid RBAM for Critical Asset identification pursuant to CIP-002-3.	Option 1
Use the CIP V5 “High” and “Medium” Impact Rating Criteria (CIP-002-5.1, Attachment 1) to identify assets subject to the controls in the CIP V5 Standards.	Option 2

Each Responsible Entity must identify the approach it is using for asset identification during the Transition Period as part of its response to a pre-Compliance Audit Survey, a pre-Spot Check data request, or as otherwise requested by the NBEUB or NPCC pursuant to the NB CMEP.

Responsible Entities using Option 1 must comply with all aspects of CIP-002-3 Requirement R1, including documentation of an RBAM that includes procedures and evaluation criteria. For Responsible Entities using Option 2, compliance with the CIP V5 High and Medium Impact Criteria will be treated as compliance with the CIP V3 RBAM requirements. Identification of Critical Assets (or BPS Cyber Assets under the CIP V5 Standards) will then follow that chosen criteria as described below.

For Responsible Entities using Option 2, the types of assets defined in CIP-002-3 Requirements R1.2.1 through R1.2.6 should be assessed against the Impact Rating Criteria, using the asset characteristics defined in each Criterion as the evaluation criteria. The results of this application will result in a list of assets matching High, Medium, and/or Low Impact criteria. Any asset matching one or more High or Medium Impact criteria will be deemed Critical Assets for the purposes of compliance with CIP-002-3 Requirement R2. Any asset matching only Low Impact criteria will not be considered a Critical Asset.

Regardless of the option the Responsible Entity chooses, it must be compliant with the requirements of Reliability Standard CIP-002-5.1 on the effective date of the CIP V5 Standards as discussed in this document.

4. Newly Identified Critical Cyber Assets

In accordance with the approach set forth above, during the Transition Period a Responsible Entity with newly identified systems and facilities may begin implementing the CIP V5 Standards for such systems and facilities. This allows Responsible Entities that will be implementing new systems or that have newly identified assets applicable to the CIP V5 Standards a clear path to transition to the CIP V5 Standards without the added compliance burden of first complying with the CIP V3 Standards during the Transition Period.

If a Responsible Entity's application of the CIP V5 Impact Rating Criteria identifies a system or facility that would be categorized as a BPS Cyber System under the CIP V5 Standards but would not be considered a Critical Cyber Asset under the CIP V3 Standards, the requirements of the CIP V5 Standards will be enforced on the effective date of the CIP V5 Standards. If, on the other hand, the newly identified asset would be a BPS Cyber System under the CIP V5 Standards and a Critical Cyber Asset under the CIP V3 Standards, Responsible Entities must be compliant with the CIP Reliability Standards (either the CIP V3 or the CIP V5 Standards, at the Responsible Entity's discretion) during the Transition Period.

Additionally, during the Transition Period planned changes to existing Critical Cyber Assets must be compliant with the CIP Reliability Standards (either the CIP V3 or the CIP V5 Standards) upon commissioning. This includes replacement of existing Critical Cyber Assets (e.g., a SCADA/EMS upgrade or replacement). Similarly, changes to "non-Critical" Cyber Assets at a previously identified Critical Asset (from the application of a CIP V3 RBAM) must be compliant with the CIP Reliability Standards (either the CIP V3 or the CIP V5 Standards) upon commissioning if the change would result in the Cyber Asset being identified as a Critical Cyber Asset. For example, converting an existing Critical Asset substation protective relay from using a non-routable to a routable communication protocol would result in a Cyber Asset becoming a Critical Cyber Asset.⁵

5. Compliance Monitoring During the Transition Period

During the Transition Period, the NBEUB and NPCC will continue to conduct audits to assess compliance with the CIP Reliability Standards. For those Responsible Entities that do not have any Critical Assets or Critical Cyber Assets under the CIP V3 Standards, however, the NBEUB will forgo off-site audits of the CIP Reliability Standards during the Transition Period. The NBEUB may instead use compliance monitoring methods, such as Spot Checks, Self-Certifications, among others.

Responsible Entities with CIP audits scheduled to occur before the effective date of the CIP V5 Standards will be expected to notify the NBEUB and NPCC of whether:

1. The Responsible Entity has begun the early adoption process for the CIP V5 Standards and, if so, for which CIP V5 requirements, or
2. The Responsible Entity has not begun the early adoption process for the CIP V5 Standards and will demonstrate compliance with the CIP V3 Standards without regard to the CIP V5 Standards.

⁵ This provision does not apply to any Critical Cyber Asset at a Critical Asset identified as a result of applying the CIP Version 5 Impact Rating Criteria.

The Responsible Entity must make this notification within 15 days of receipt of a Request for Information (“RFI”) from the NBEUB or NPCC, as follows. The NBEUB or NPCC will provide the RFI to the Responsible Entity 45 days prior to the normal 60-day audit notification letter (i.e., 105 days before the audit). The RFI will include a spreadsheet listing the requirements in the Compatibility Tables. The Responsible Entity will be expected to return the completed spreadsheet to the NBEUB and NPCC within 15 days of receipt noting whether it has begun the early adoption of a CIP V5 requirement or whether it will demonstrate compliance with the CIP V3 requirement without regard to the CIP V5 Standards.

The NBEUB understands that an audit may occur while a Responsible Entity is in the course of transitioning multiple locations or facilities to compliance with a CIP V5 requirement and that all such locations or facilities may not be at the same stage of CIP V5 implementation. In that case, the declaration sent to the NBEUB and NPCC should define by category, location, or requirement where CIP V5 or CIP V3 requirements should apply, or should otherwise make clear to the NBEUB and NPCC where disparities in applying CIP V5 or CIP V3 requirements exist.

As described above, for audits of a Responsible Entity that has notified the NBEUB and NPCC that it has begun to adopt some or all of the CIP V5 Standards, if the NBEUB and NPCC finds that the Responsible Entity is generally satisfying a CIP V5 requirement, the Responsible Entity will be deemed to have no findings of non-compliance with the compatible CIP V3 requirement without further review. If the auditor finds that the Responsible Entity has not satisfied the CIP V5 requirement, however, the auditors will review whether the Responsible Entity is compliant with the compatible CIP V3 requirement. If the auditors find that the Responsible Entity has also failed to comply with the CIP V3 requirement, the NBEUB may initiate an enforcement action in accordance with the New Brunswick Compliance Monitoring and Enforcement Program.

The NBEUB’s expectations with respect to self-reports during the Transition Period will reflect its flexible compliance monitoring and enforcement approach. Specifically, if a Responsible Entity transitions to compliance with a CIP V5 requirement, the NBEUB does not expect the Responsible Entity to maintain a compliance program for the compatible CIP V3 requirement and self-report occurrences of non-compliance with the CIP V3 requirement. Rather, the Responsible Entity should focus on implementing the CIP V5 Standards and may self-identify any failures to meet the obligations of a CIP V5 requirement to which it has transitioned.

6. Technical Feasibility Exceptions (“TFEs”)

This section discusses how the NBEUB will treat TFEs during the Transition Period. In general, TFEs will align with the overall transition process from the CIP V3 Standards to the CIP V5 Standards and will be considered in the context of the underlying requirement(s).

Specifically, for TFEs available under the CIP V5 Standards that are compatible to TFEs available under the CIP V3 Standards, as of the effective date of the CIP V5 Standards, Responsible Entities must simply update the appropriate requirement references and modify the applicable mitigation plans, as necessary, to continue their TFEs. Responsible Entities may begin this process by submitting updates and modifications via a Material Change Report. The table below lists the TFEs available under the CIP V5 Standards that are compatible with TFEs available under the CIP V3 Standards.

V5 TFEs Compatible to V3 TFEs	
V5	V3
CIP-005-5 R2.3	CIP-005-3a R2.4
CIP-007-5 R1.1	CIP-007-3a R2.3
CIP-007-5 R4.3	CIP-007-3a R6.4
CIP-007-5 R5.6	CIP-007-3a R5.3.3

If a system or device is unable to meet strict compliance with a CIP V5 requirement but has no compatible TFE under the CIP V3 Standards, a Responsible Entity may submit a new TFE request. A Responsible Entity should contact the NBEUB for guidance regarding those TFE requests. The table below lists the TFEs available under the CIP V5 Standards that are not compatible with TFEs available under the CIP V3 Standards.

V5 TFEs Not Compatible with V3 TFEs			
CIP-005-5	CIP-006-5	CIP-007-5	CIP-010-1
R1.4	R1.3	R5.1	R1.5
R2.1		R5.7	R3.2
R2.2			

Existing TFEs under the CIP V3 Standards that are no longer applicable under the CIP V5 Standards may be maintained throughout the Transition Period as a safe harbor even if the Responsible Entity transitions to implementing the relevant CIP V5 requirement. The table below lists the TFEs available under the CIP V3 Standards that are not applicable under the CIP V5 Standards.

V3 TFEs Not Applicable Under V5		
CIP-005-3a	CIP-006-3c	CIP-007-3a
R3.1	R1.1	R3.2
R3.2		R4
		R5.3
		R5.3.1
		R5.3.2
		R6

7. Conclusion

This Compliance Guidance Statement has been established to promote a smooth transition to the CIP V5 Standards. Responsible Entities may submit questions relating to this Compliance Guidance Statement to Compliance@nbeub.ca.