



January 6, 2020

VIA ELECTRONIC FILING

Honorable Kimberly D. Bose, Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: ISO New England Inc., Docket No. ER20-____-000;
Cost Recovery Mechanism for Facilities Designated Critical to the
Derivation of Interconnection Reliability Operating Limits**

Dear Secretary Bose:

Pursuant to Section 205 of the Federal Power Act,¹ ISO New England Inc. (the “ISO”)² hereby submits proposed revisions to the ISO’s OATT to incorporate a mechanism that facilitates the recovery of critical infrastructure protection (“CIP”) costs by facilities that the ISO identifies as critical to the derivation of Interconnection Reliability Operating Limits (“IROL”).³ The proposed cost recovery mechanism is reflected in a new Schedule 17 – Recovery of Critical Infrastructure Protection Costs by Facilities Critical to the Derivation of Interconnection Reliability Operating Limits – of the OATT (“Schedule 17”). The proposed revisions to the OATT discussed in this transmittal letter are collectively referred to as the “IROL-CIP Cost Recovery Rules.” This filing also includes the supporting testimonies of Jonathan B. Lowell (the “Lowell Testimony”), Dean L. LaForest (the “LaForest Testimony”), and Ingrid Rayo (the “Rayo Testimony”).⁴

¹ 16 U.S.C. § 824d (2006 and Supp. II 2009).

² Capitalized terms used but not otherwise defined in this filing letter have the meanings ascribed thereto in the ISO’s Transmission, Markets and Services Tariff (the “Tariff”). Section II of the Tariff contains the Open Access Transmission Tariff (the “OATT”).

³ See Tariff at § I.2.2 (defining IROL as having “the meaning specified in the Glossary of Terms Used in NERC Reliability Standards). See Glossary of Terms Used in NERC Reliability Standards, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (last visited January 3, 2020) (“NERC Glossary of Terms”).

⁴ Mr. Lowell is a Principal Analyst in the Market Development Department of the ISO. Mr. La Forest is Manager, Real-Time Studies in the System Operations Department of the ISO. Ms. Rayo is a Senior Reliability Consultant

The ISO submits that the IROL-CIP Cost Recovery Rules are just and reasonable. As more fully discussed in Section III of this transmittal letter, Bulk Electric System (“BES”⁵) generation and transmission facilities (*e.g.*, merchant transmission facilities) that are identified by the ISO as critical to the derivation of IROLs (“IROL-Critical Facilities”) must comply with the North American Electric Reliability Corporation (“NERC”) Critical Infrastructure Protection (“CIP”) Reliability Standards’ requirements for medium impact BES Cyber Systems.⁶ The requirement for IROL-Critical Facilities to meet these higher standards imposes additional costs on these facilities. These costs, however, are incurred only by a limited subset of the resources in the region – specifically, by 27 generation units at 15 plant locations and by one merchant transmission facility.⁷ Those that incur these costs thus operate under an externally imposed financial disadvantage relative to other, similar resources with which they compete in the New England wholesale markets. Therefore, with this proposal, the ISO is providing a simple mechanism that owners of IROL-Critical Facilities (“IROL-Critical Facility Owners”) may use to recover Commission-approved incremental costs to comply with NERC CIP Standards’ requirements for medium impact assets. Providing a mechanism to facilitate the recovery of IROL-CIP Costs is consistent with and furthers the Commission’s long-standing policy to enable the recovery of prudently-incurred, reliability-related costs, including those related to compliance with mandatory NERC CIP standards.⁸

The ISO respectfully requests that the Commission accept the IROL-CIP Cost Recovery Provisions as filed, without modifications or conditions, to be effective March 6, 2020, which is sixty days from the date of this filing.

I. DESCRIPTION OF THE FILING PARTY AND COMMUNICATIONS

The ISO is the independent, private, non-profit entity that serves as the Regional Transmission Organization (“RTO”) for New England. The ISO operates the New England bulk power system and administers New England’s organized wholesale electricity market pursuant to the ISO New England Transmission, Markets and Services Tariff and the Transmission Operating Agreement with the New England Participating Transmission Owners. In its capacity

with Burns & McDonnell Engineering, a consulting firm engaged by the ISO to support the IROL-CIP Cost Recovery Rules.

⁵ BES is defined in the NERC Glossary of Terms.

⁶ See *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization*, North American Reliability Corporation, <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf> (last visited January 3, 2020) (requiring the identification, assessment and categorization of BES Cyber Systems and associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that their loss, compromise or misuse could have on the reliable operation of the BES) (“CIP-002-5.1”). Criterion 2.6 in Attachment A – Impact Rating Criteria to CIP-002-5.1 assigns a medium impact rating to generation and transmission facilities identified as IROL-Critical Facilities.

⁷ See LaForest Testimony at 6.

⁸ See *PJM Interconnection, L.L.C.*, 138 FERC ¶ 61,020 at P 50 (2012) (referencing the Commission’s policy in considering a proposal to allow for recovery of blackstart costs, including NERC CIP compliance). See also *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, 96 FERC ¶ 61,229 at 61,129 (2001).

as an RTO, the ISO has the responsibility to protect the short-term reliability of the New England Control Area and to plan and operate the system according to reliability standards established by the Northeast Power Coordinating Council, Inc. (“NPCC”) and the NERC. In particular, the ISO is the NERC Reliability Coordinator for the New England Reliability Coordinator Area/Balancing Authority Area (“RCA/BAA”).

All correspondence and communications in this proceeding should be addressed to the undersigned for the ISO:

Monica Gonzalez, Esq.
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040-2841
Tel: (413)535-4178
Fax: (413) 535-4379
Email: mgonzalez@iso-ne.com

II. STANDARD OF REVIEW

The IROL-CIP Cost Recovery Rules are submitted pursuant to Section 205 of the FPA, which “gives a utility the right to file rates and terms for services rendered with its assets.”⁹ Under Section 205, the Commission “plays ‘an essentially passive and reactive’ role”¹⁰ whereby it “can reject [a filing] only if it finds that the changes proposed by the public utility are not ‘just and reasonable.’”¹¹ The Commission limits this inquiry “into whether the rates proposed by a utility are reasonable – and [this inquiry does not] extend to determining whether a proposed rate schedule is more or less reasonable than alternative rate designs.”¹² The IROL-CIP Cost Recovery Rules filed herein “need not be the only reasonable methodology, or even the most accurate.”¹³ As a result, even if an intervenor or the Commission develops an alternate proposal, the Commission must accept this Section 205 filing if it is just and reasonable.¹⁴

⁹ *Atlantic City Elec. Co. v. FERC*, 295 F.3d 1, 9 (D.C. Cir. 2002).

¹⁰ *Id.* at 10 (quoting *City of Winnfield v. FERC*, 744 F.2d 871, 876 (D.C. Cir. 1984)).

¹¹ *Id.* at 9.

¹² *Cities of Bethany, Bushnell et al. v. FERC*, 727 F.2d 1131, 1136 (D.C. Cir.), *cert. denied*, 469 U.S. 917 (1984) (“*Cities of Bethany*”); *see also ISO New England Inc.*, 114 FERC ¶ 61,315 at P 33 and n.35 (2005), *citing Pub. Serv. Co. of New Mexico v. FERC*, 832 F.2d 1201, 1211 (10th Cir. 1987) and *Cities of Bethany* at 1136.

¹³ *Oxy USA, Inc. v. FERC*, 64 F.3d 679, 692 (D.C. Cir. 1995) (citing *Cities of Bethany* at 1136).

¹⁴ *Cf. Southern California Edison Co., et al.*, 73 F.E.R.C. ¶ 61,219 at 61,608 n.73 (1995) (“Having found the Plan to be just and reasonable, there is no need to consider in any detail the alternative plans proposed by the Joint Protesters.”) (citing *Cities of Bethany* at 1136).

III. BACKGROUND

A. IROL-Critical Facilities' Requirement to Comply with CIP Standards' Requirements for Medium Impact Assets

On November 22, 2013, in Order No. 791, the Commission approved version 5 of the CIP Cyber Security Standards, including Reliability Standard CIP-002-5.1.¹⁵ CIP version 5 standards included a revised methodology for categorizing BES Cyber Assets which incorporated mandatory protections for all high, medium, and low impact BES Cyber Assets. As relevant here, the CIP version 5 standards require responsible entities (such as IROL-Critical Facility Owners) to identify and categorize each of their BES Cyber Systems according to specific criteria (low, medium, high) set forth in Attachment 1 – Impact Rating Criteria of CIP-002-5.1. These standards categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of each BES Cyber System could have on the reliable operation of the BES.¹⁶ Once a BES Cyber System is categorized, the responsible entity must comply with the requirements of the CIP version 5 standards that apply to the facility's impact category.

Under the CIP version 5 standards, all BES Cyber Systems, at a minimum, must be categorized as low impact assets. Section 2 of Attachment 1, however, assigns a medium impact rating to certain generation and transmission facilities, including:

Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.¹⁷

As briefly discussed below, the ISO identifies or designates certain generation and transmission facilities as IROL-Critical Facilities pursuant to applicable NERC Reliability Standards and system operating procedures. The facilities that the ISO so designates as critical to the derivation of IROLs must comply with CIP standards corresponding to the medium impact category.¹⁸

¹⁵ *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 at PP 41, 87 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014). Order No. 791 became effective February 3, 2014.

¹⁶ *See* Order No. 791 at PP 14, 20. *See also* CIP-002-5.1 at § A.3.

¹⁷ CIP-002-5.1 at Att. 1, § 2.

¹⁸ For clarity, the ISO determines whether a generation or transmission facility is critical to the derivation of an IROL pursuant to the ISO's System Operating Limit ("SOL") methodology. If a facility is found to be critical to the derivation of an IROL, under CIP-002-5.1, the respective responsible entity assesses its BES Cyber Assets and designates them as medium impact BES Cyber Systems. Under the CIP Cyber Security Standards,

[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber Systems. For example,

Pursuant to the implementation plan approved in Order No. 791, responsible entities had to achieve compliance by April 1, 2016 for provisions pertaining to medium impact assets.¹⁹

B. IROL-Critical Facilities' Request for Mechanism to Recover Reliability-Related Costs Solely Due to ISO's IROL-Critical Facility Designation

In accordance with applicable NERC Reliability Standards, the ISO, as the Reliability Coordinator, is required to ensure that System Operating Limits, including IROLs, for the New England RCA/BAA are established and are consistent with the ISO's SOL methodology.²⁰ Pursuant to that methodology, the ISO determines whether a generation or transmission facility is critical to the derivation of an IROL.²¹ IROL, as defined by NERC, is an SOL "that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System."²²

As Mr. LaForest explains in his testimony, the ISO has been identifying transmission facilities since 2013 and generation facilities since 2014 as IROL-Critical Facilities pursuant to the ISO's SOL methodology in accordance with NERC Reliability Standards.²³ The ISO designates as IROL-Critical Facilities those generation and transmission facilities that the ISO has found, through system modeling and analysis, to be impactful to IROLs under certain conditions.²⁴ Whether a generation or transmission facility is critical to an IROL derivation,

the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems.

See CIP-002-5.1 at § 6. The responsible entity has to protect what it designates as medium impact BES Cyber Systems.

¹⁹ See Order No. 791 at P 171. See also Order No. 791-A at PP 10-12.

²⁰ See LaForest Testimony at 45. See also *FAC-011-3 – System Operating Limits Methodology for the Operating Horizon*, North American Reliability Corporation, <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf> (last visited January 3, 2020) (requiring Reliability Coordinators to establish a methodology for use in developing SOLs within the Reliability Coordinator Area, including criteria for determining when an SOL qualifies as an IROL); *FAC-014-2 – Establish and Communicate System Operating Limits*, North American Reliability Corporation, <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf> (last visited January 3, 2020) (requiring Reliability Coordinators to ensure the SOLs, including IROLs, are established pursuant to SOL methodology, and provide the identification of facilities that are critical to the derivation of an IROL). The ISO's SOL methodology for operational planning and real-time operations for the New England RCA/BAA is documented in the ISO's *Master/Local Control Center Procedure No. 15 (M/LCC 15) System Operating Limits Methodology*, available at https://www.iso-ne.com/static-assets/documents/rules_proceeds/operating/mast_satllte/mlcc15.pdf.

²¹ See LaForest Testimony at 4-5.

²² See NERC Glossary of Terms.

²³ See La Forest Testimony at 4-5.

²⁴ See *id.*

depends on a number of factors, including its location on the system.²⁵ Generation and transmission facilities may become part of or create a new IROL condition based on New England Transmission System changes, such as the addition of transmission facilities or the addition of new or the retirement of existing generation facilities.²⁶ Likewise, system changes may result in the termination of a facility's previous designation as an IROL-Critical Facility. The ISO reviews IROL-Critical Facility designations annually or more frequently if warranted by significant changes on the system.²⁷ When the ISO identifies a generation or transmission facility as critical to the derivation of IROLs, it provides written notification of the designation to the facility owner (or the associated Market Participant).²⁸

Stakeholder representatives of generation and similarly-situated merchant transmission facilities that have been designated as IROL-Critical Facilities asked the ISO to consider and include in its work plans the development of a mechanism for recovery of the costs they must incur to comply with the higher reliability standards associated with the ISO's designation as IROL-Critical Facilities. The obligation of IROL-Critical Facility Owners to comply with CIP standards corresponding to the medium impact category arises from the ISO's designation, and is not within the IROL-Critical Facility's control.²⁹ Designation as an IROL-Critical Facility can lead to additional costs for such facilities, costs that are not typically incurred by operators of other resources and facilities, but which relate to ensuring a more reliable electric grid for all users of the BES in the New England region.³⁰

The Commission's long-standing policy has been to facilitate the recovery of prudently incurred, reliability-related costs, including those related to compliance with mandatory NERC CIP standards.³¹ However, as Mr. Lowell explains in his testimony, IROL-Critical Facility Owner's costs to comply with the CIP medium impact standards place them at a financial disadvantage relative to the other resources with which they compete in the New England Markets.³² Therefore, in furtherance of the Commission's policy, the ISO developed a simple mechanism to facilitate the recovery of these reliability-related costs through the ISO Tariff. The ISO's cost recovery approach and the rules created to implement that approach are described below.

²⁵ See *id.* at 5.

²⁶ See *id.* at 6.

²⁷ See *id.*

²⁸ See LaForest Testimony at 6-7.

²⁹ See *id.* at 7.

³⁰ See Lowell Testimony at 7.

³¹ See *PJM Interconnection, L.L.C.*, 138 FERC at P 50.

³² See Lowell Testimony at 7. Note, as Mr. LaForest explains, there are other facilities in New England that meet other criteria under Section 2 of Attachment 1 to CIP-002-5.1 for medium impact assets. See LaForest Testimony at 8. The ISO's proposal, however, focuses only on IROL-Critical Facilities – a designation that is due to circumstances that are entirely outside of the IROL-Critical Facility Owner's control.

IV. DESCRIPTION AND RATIONALE FOR PROPOSED TARIFF CHANGES

The IROL-CIP Cost Recovery Rules set forth in new Schedule 17 of the ISO's OATT provide a vehicle for an IROL-Critical Facility Owner to recover IROL-CIP Costs as and to the extent accepted by the Commission upon an owner's submission of an appropriate filing under Section 205 of the FPA. Under the proposed mechanism, the ISO will act as agent to bill, collect, and remit to IROL-Critical Facility Owners such owners' Commission-accepted incremental costs to comply with NERC CIP standards' medium impact requirements for designated IROL-Critical Facilities. The ISO will charge such costs to Transmission Customers receiving Regional Transmission Service following an IROL-Critical Facility Owner's notification to the ISO of an order of the Commission accepting the owner's IROL-CIP Costs. The IROL-CIP Cost Recovery Rules incorporate certain procedural and information requirements intentionally designed to provide structure for, and otherwise to facilitate and narrow the scope of, what may be multiple resource owners' Section 205 filings for recovery of such costs, and thus reduce potential controversy regarding such filings.

A key component of the IROL-CIP Cost Recovery Rules is the new Schedule 17 of the ISO's OATT. Schedule 17 is comprised of three key sections and an Attachment A. Section 1 discusses the ISO's process for designating and notifying IROL-Critical Facilities. Section 2 discusses the eligibility requirements for cost recovery through Schedule 17, including pre-filing requirements and parameters for IROL-Critical Facility Owners' individual Section 205 filings. Section 3 describes the ISO's authorization to charge and disburse Commission-accepted IROL-CIP Costs, and the allocation of costs to Transmission Customers. Attachment A lists the cost categories associated with compliance with NERC CIP standards applicable to medium impact BES Cyber Systems to standardize (and, thereby, facilitate) individual IROL-Critical Facility Owners' Section 205 filings. These sections are described further below, and the specifics of the proposed mechanism are detailed in the supporting testimonies.

A. IROL-CIP Costs Eligible for Recovery Under Schedule 17

Schedule 17 provides for the recovery of an IROL-Critical Facility Owner's IROL-CIP Costs. Under the proposed rules, "IROL-CIP Costs" means an IROL-Critical Facility Owner's incremental capital, operation and maintenance, and associated administrative and regulatory costs of complying with NERC CIP standards corresponding to the medium impact category at one or more IROL-Critical Facilities, to the extent those costs have been accepted by the Commission.³³ "Incremental costs" refers to additional costs paid in excess of the costs the

³³ Schedule 17 specifies the IROL-CIP Costs that are eligible for recovery in the "Introduction" and in Section 2.2(A), which lists IROL-CIP Costs as those that:

(i) are incurred by the IROL-Critical Facility Owner during the period in which the subject facility is designated as an IROL-Critical Facility; (ii) are paid by the IROL-Critical Facility Owner during the cost recovery period specified by the IROL-Critical Facility Owner in the Table 1 provided in Attachment to this Schedule 17; (iii) are presented by the IROL-Critical Facility Owner in a Section 205 filing and approved by the Commission; and (iv) satisfy all other conditions for recovery, as set forth in this Schedule 17.

facility owner otherwise would have incurred to meet the CIP standards' low impact requirements. The proposal limits IROL-CIP Costs to those that have been paid – not just committed for future payment – to avoid the potential controversy regarding those projects and facilitate a streamlined, less litigious option for cost recovery. Finally, to ensure against double recovery, the proposed revisions explicitly exclude from recovery under Schedule 17 any costs already subject to recovery under another provision of the Tariff or under any contractual arrangement to which the IROL-Critical Facility Owner is a party.

B. Process for Designating/Terminating IROL-Critical Facilities and Notifying IROL-Critical Facility Owners

The Schedule 17 cost recovery mechanism will be available only to IROL-Critical Facilities. As such, Section 1 of Schedule 17 describes the process for notifying an IROL-Critical Facility Owner (or its Lead Market Participant, where appropriate) when its generation or transmission facility has been designated as an IROL-Critical Facility and when changes to that designation occur based on the ISO's review. In these notifications, the ISO will identify the facility designated as an IROL-Critical Facility and the effective date of the designation (or termination of same). This notification, in turn, will provide the foundation for IROL-Critical Facility Owners' representations of their designated status in their respective Section 205 filings for recovery of IROL-CIP Costs.

C. Eligibility Requirements to Recover IROL-CIP Costs Under Schedule 17

1. Section 205 Filing Requirement

Section 2 of Schedule 17 sets forth the proposed eligibility requirements for recovery of IROL-CIP Costs through the Schedule 17 mechanism. Under the ISO's proposal, an IROL-Critical Facility Owner must submit a filing to the Commission pursuant to Section 205 of the FPA requesting approval of IROL-CIP Costs that it proposes to recover under Schedule 17. While this approach can result in multiple FPA Section 205 filings, it is consistent with Order No. 679, which clarified that the Commission would "review applications for the recovery of such prudently incurred costs under its section 205 procedures," and that, "ultimately, the burden is on the applicant to demonstrate that its proposal is just and reasonable."³⁴ It is also consistent with existing mechanisms in the ISO's Tariff that allow for recovery of costs pursuant to FPA Section 205 filings.³⁵

³⁴ See Order No. 679 at PP 343, 347.

³⁵ See Tariff, Section II, Schedules 13 and 14; *id.* at § III.A.15.2.

Importantly, these requirements apply only to the extent the IROL-Critical Facility Owner wishes to recover its costs through Schedule 17. However, nothing in Schedule 17 restricts or limits the rights of an IROL-Critical Facility Owner to make a filing with the Commission pursuant to Section 205 of the FPA, at any time, to recover reliability-related compliance costs through a means other than Schedule 17. Nevertheless, the ISO anticipates that the relative simplicity of Schedule 17 will be attractive to IROL-Critical Facility Owners, and will minimize litigation through its pre-filing review process and identification of general categories of IROL-CIP Costs for IROL-Critical Facility Owners to use in their Section 205 filings.

2. Pre-Filing Requirements

Section 2.1 of Schedule 17 sets forth a light pre-filing construct designed to provide interested parties an opportunity to meaningfully review and understand an IROL-Critical Facilities Owner's IROL-CIP Costs before they are filed with the Commission for approval. This feature was of significant import to stakeholders. Having this upfront opportunity to review and understand proposed IROL-CIP Costs may help to avoid or minimize expensive and protracted litigation of individual Section 205 filings before the Commission.

The proposed pre-filing review process includes four simple elements.³⁶ First, under Section 2.1(A) of Schedule 17, the IROL-Critical Facility Owner is required to provide to the ISO a non-confidential summary description of the proposed filing, including the IROL-CIP Costs and supporting data, calculations and workpapers, and the IROL-Critical Facility Owner's contact information.³⁷ Second, Section 2.1(A) requires the ISO to post on its website all materials provided to the ISO by the IROL-Critical Facility Owner, and to provide notice of the posting to all entities that self-subscribe to a distribution list specifically created for dissemination of Schedule 17 information. Third, Section 2.1(B) of the new schedule requires the IROL-Critical Facility to host, no sooner than 15 days after the ISO's posting, an interactive

³⁶ See Tariff at § III.A.15.2 (providing for IMM's pre-filing review of Section 205 filings for additional fuel and operating and maintenance costs).

³⁷ Under the ISO's Information Policy in Attachment D to the Tariff and Critical Energy Infrastructure ("CEII") implementation policy, the naming of an IROL-Critical Facility alone does not rise to the level of Confidential Information as it is not commercially sensitive information, or CEII treatment absent additional details describing a bulk electric system vulnerability (*e.g.*, specific conditions and contingencies rendering the facility critical along with descriptions of the consequences of those contingencies). While the ISO does not classify the name of an IROL-Critical Facility itself as Confidential Information or CEII, IROL-Critical Facility Owners should not release and should take all appropriate measures to protect information that, in combination with the identity of the facility, would be Confidential Information, CEII, or otherwise could jeopardize the security or reliable operation of the system. Such information may include, but is not limited to, information about the facility that renders it critical to an IROL determination (to the extent such information is known by the IROL-Critical Facility Owner) or measures (*e.g.*, vendors, software and descriptions of communication systems and cyber security protections) employed to protect the facility in accordance with NERC's Reliability Standards. To seek privileged treatment of certain information, IROL-Critical Facility Owners must comply with the Commission's requirements for filing privileged information, including the provision of a proposed form of Non-Disclosure Agreement, in their respective Section 205 filings for IROL-CIP Costs recovery. See 18 C.F.R. § 388.112(b) (2018).

briefing session to review the IROL-CIP Costs proposed for recovery. Fourth, Section 2.1(C) requires the IROL-Critical Facility Owner to provide a 60-day review period to address interested parties' requests for additional information and concerns regarding the owner's proposed cost recovery filing. The IROL-Critical Facility Owner may extend the 60-day period at its discretion. Under Section 2.1(C), the IROL-Critical Facility Owner is free to submit its filing for IROL-CIP Costs approval pursuant to Section 205 of the FPA following the conclusion of the 60-day period. However, if there are no interested parties or interested parties inform the IROL-Critical Facility Owner that they no longer desire additional pre-filing time, the IROL-Critical Facility Owner may proceed with the filing without awaiting the end of the 60-day period.

3. Section 205 Filing Information Requirements

Section 2.2 of Schedule 17 sets out the requirements for an IROL-Critical Facility Owner's Section 205 filing for recovery of IROL-CIP Costs. Consistent with the proposed definition of IROL-CIP Costs in the Introduction of Schedule 17, Section 2.2(A) lists the IROL-CIP Costs eligible for recovery. These are costs that: (1) are incurred by the IROL-Critical Facility Owner during the period in which the subject facility is designated as an IROL-Critical Facility Owner; (2) are paid by the IROL-Critical Facility Owner during the cost recovery period specified by the IROL-Critical Facility Owner in Table 1 provided in Attachment A to Schedule 17; (3) are filed by the IROL-Critical Facility Owner under FPA Section 205 and accepted by the Commission; and (4) satisfy all other conditions for recovery (*e.g.*, the requirements set out in Section 2) under Schedule 17.

Section 2.2(B) requires the IROL-Critical Facility Owner to conform the information supporting the proposed IROL-CIP Costs to the data requirements set forth in Table 1 provided in Attachment A to Schedule 17. The data requirements include: the identification of the specific IROL-Critical Facility; categorization of costs by function and subject matter; and specification of the cost recovery period in which the costs were paid. The Section 2.2(B) requirement is intended to facilitate IROL-Critical Facility Owners' individual Section 205 filings, and provide a standard format for the costs to be presented.

Attachment A identifies the general IROL-CIP Cost categories for use in individual Section 205 filings. As Mr. Lowell's testimony explains, the ISO itself does not have expertise regarding the types of direct costs commonly associated with IROL-Critical Facilities' compliance with CIP standards' medium impact requirements.³⁸ However, to facilitate IROL-Critical Facility Owners' filings, the ISO engaged Ms. Rayo of Burns and McDonnell, a consulting engineering firm with broad experience in the electricity industry, to identify the medium impact BES Cyber System requirements and the types of direct costs associated with compliance with those requirements.³⁹ The proposed Table 1 in Attachment A to Schedule 17

³⁸ See Lowell Testimony at 6.

³⁹ See *id.*

reflects the categories identified in the Rayo Testimony as reasonable and appropriate direct costs for recovery under Schedule 17.⁴⁰ The direct cost primary categories include: facility staff labor; compliance staff labor; other labor; equipment costs; software/applicable license, maintenance and support, and upgrade costs; outside services and fees; physical improvement costs; and production, printing, and shipping costs.⁴¹

Additionally, Attachment A recognizes that there may be other, direct or indirect costs that do not fit within the direct cost categories, but which may arise from or be associated with an IROL-Critical Facility Owner's compliance with medium impact BES Cyber System requirements. As Ms. Rayo's testimony explains, costs directly related to compliance that do not fit into the predefined categories may include lodging, food or transport costs.⁴² In addition to the costs identified by Ms. Rayo, the ISO recognizes that there may be other costs (*e.g.*, administrative and regulatory costs)⁴³ that are indirectly associated with compliance.⁴⁴ Therefore, Attachment A includes an "Other" category, which IROL-Critical Facility Owners may use for those types of costs. While Attachment A identifies the categories of costs commonly observed as necessary to support a cybersecurity program for medium impact BES Cyber Systems, such as IROL-Critical Facilities, each individual IROL-Critical Facility Owner will still need to justify the application of the cost categories and the corresponding costs at its IROL-Critical Facility in any Section 205 filing it elects to submit pursuant to Schedule 17.

Finally, the proposed Section 2.2(C) of Schedule 17 provides an IROL-Critical Facility Owner the flexibility to submit an individual Section 205 filing at any interval that is at least 12 months subsequent to a previous filing (subject to satisfying the Schedule 17 pre-filing requirements), instead of prescribing a fixed filing schedule. This flexibility should help avoid multiple, simultaneous filings by various IROL-Critical Facility Owners, and thus should improve the overall efficiency of the Schedule 17 cost recovery mechanism. This feature affords IROL-Critical Facility Owners the flexibility to balance the frequency of their Section 205 filings (*e.g.*, 12 months, 24 months, 36 months, etc.) with the efforts involved in making those filings.⁴⁵

⁴⁰ See Rayo Testimony at 11-15.

⁴¹ See *id.* at 13-14.

⁴² See *id.* at 14-15.

⁴³ See, *e.g.*, Tariff at § III.A.15.2(iv).

⁴⁴ See Lowell Testimony at 6

⁴⁵ Requiring IROL-Critical Facility Owners to submit Section 205 filings – as opposed to, for example, annual informational updates pursuant to an established formula rates – for Commission review and acceptance also helps minimize future refund uncertainties that could be introduced by potential FPA Section 206 proceedings challenging informational rate updates, and increases regulatory certainty over IROL-CIP Costs before they are charged to Transmission Customers.

D. Invoicing and Collecting IROL-CIP Costs; Cost Allocation of IROL-CIP Costs

Section 3 of Schedule 17 incorporates the proposed rules for allocating, invoicing and collecting Commission-accepted IROL-CIP Costs from Transmission Customers receiving Regional Transmission Service, and the payment of those costs in equivalent amounts to the pertinent IROL-Critical Facility Owner(s).

Specifically, the proposed Section 3.1 requires the ISO to initiate payment of IROL-CIP Costs to the IROL-Critical Facility Owner after the IROL-Critical Facility Owner notifies the ISO that the Commission has issued an order accepting the IROL-CIP Costs for recovery.⁴⁶ The ISO will pay the Commission-accepted IROL-CIP Costs in equal monthly installments to the applicable Market Participants based on their respective ownership shares in an associated IROL-Critical Facility. Payment of the IROL-CIP Costs over a defined monthly period is intended to avoid “rate shock” to Transmission Customers that could result from a single lump sum payment.⁴⁷ The first monthly payment will be reflected in the Monthly Statement associated with the first month immediately following the ISO’s receipt of the IROL-Critical Facility Owner’s notification of the Commission’s order accepting the IROL-CIP Costs for recovery under Schedule 17.

Section 3.2 proposes to collect the total Commission-accepted IROL-CIP Costs through regional rates charged to Transmission Customers receiving Regional Network Service or Through or Out Service (except Coordinated External Transactions (“CET”))⁴⁸ over a 12-month period. Section 3.2 sets out a formula for calculating the charge to each Transmission Customer. Under the proposal, each Transmission Customer will pay monthly a pro rata share of the total IROL-CIP Costs in a month, based on the customer’s monthly Regional Network Load or average monthly Through or Out Service reservation.

⁴⁶ It is the ISO’s intention that such payments will commence after the amount of IROL-CIP Costs to be recovered is definitively established. Thus, should the Commission accept an IROL-Critical Facility Owner’s Schedule 17 filing subject to a compliance condition affecting the amount of costs the owner may recover, an order on the affected owner’s compliance filing will be the trigger for the ISO’s payment obligation under Schedule 17.

⁴⁷ See Lowell Testimony at 13.

⁴⁸ The ISO’s proposal excludes CETs receiving Through or Out Service from the allocation of IROL-CIP Costs, consistent with the existing rules exempting ETs from Through or Out Service charges. See *ISO New England Inc. and New England Power Pool*, Coordination Agreement, Market Rule 1, OATT Conforming Revisions Relating to Coordinated Transaction Scheduling, Trans. Ltr. at 24-25, Docket No. ER15-2641-000 (Sept. 10, 2015) (eliminating Through or out Service charges to support the effort to reduce cross-border transaction costs, consistent with the Coordinated Transaction Scheduling design objective to help ensure more efficient trade between the regions). See also *ISO New England Inc. and New England Power Pool*, 153 FERC ¶ 61,159 (2010) (conditionally accepting Coordinated Transaction Scheduling conforming revisions).

The ISO's proposed allocation of IROL-CIP Costs to Transmission Customers is consistent with the Commission's cost allocation principles,⁴⁹ and thus appropriate. IROL-CIP Costs directly arise from IROL-Critical Facility Owners' compliance with CIP standards applicable to medium impact BES Cyber Systems to ensure the reliable operation of the New England Transmission System. These standards require IROL-Critical Facility Owners to protect their facilities against events or threats for the benefit of the system. As Mr. LaForest's testimony explains, IROL-Critical Facility Owners' compliance with CIP standards allows the ISO to operate the system with higher limits without unacceptable risk.⁵⁰ Conversely, compromised IROL-Critical Facilities' controls, for example, can lead to inadvertent operation of the system using incorrect limits.⁵¹ Operating the system based on faulty limits can result in local or wide-spread system instabilities, potentially leading to uncontrolled separation, cascading outages, and blackouts in the New England and neighboring control areas.⁵² Additionally, the proposed allocation of IROL-CIP Costs to Transmission Customers is consistent with the cost allocation for other traditional transmission-related reliability needs, including that used for VAR Service under Schedule 2 of the OATT,⁵³ and proposed for CIP payments to Blackstart resources under Schedule 16 of the OATT had those resources been required to comply with CIP standards' requirements for medium impact assets.⁵⁴ Therefore, the proposed cost allocation is appropriate.

IV. STAKEHOLDER PROCESS

The ISO made its initial proposal to stakeholders at the February 20, 2019 NEPOOL Transmission Committee meeting. Stakeholder discussions (and proposed revisions) continued at the Transmission Committee meetings in March, April, May, June, August, September, and October 2019. The IROL-CIP Cost Recovery Rules proposed in this filing were not supported in votes by the Transmission Committee at its October 10, 2019 meeting or the NEPOOL Participants Committee at its November 1, 2019 meeting, due to differences as to whether IROL-CIP Costs should be subject to out-of-market cost recovery and the proposed cost allocation.

⁴⁹ See generally *Transmission Planning and Cost Allocation by Transmission Owning and Operating Public Utilities*, Order No. 1000, 136 FERC ¶ 61,051 at PP 504-508 (2011), *order on reh'g & clarification*, Order No. 1000-A, 139 FERC ¶ 61,132, *order on reh'g & clarification*, Order No. 1000-B, 141 FERC ¶ 61,044 (2012), *aff'd sub nom. S.C. Pub. Serv. Auth. V. FERC*, 762 F.3d 41 (D.C. Cir. 2014).

⁵⁰ See LaForest Testimony at 8.

⁵¹ See *id.*

⁵² See *id.*

⁵³ See Tariff, Section II, Schedule 2 at § III.

⁵⁴ See *ISO New England Inc., et al.*, Revisions to Schedule 16 of the OATT, Trans. Ltr. at 23, Docket No. ER12-729, *et al.* (filed Dec. 30, 2011). See also *ISO New England Inc., et al.*, Letter Order, Docket Nos. ER12-729-000, *et al.* (Feb. 17, 2012) (accepting revisions to Schedule 16 of the ISO's OATT, allowing for the recovery of CIP medium impact costs and charging of those cost to transmission customers).

V. REQUESTED EFFECTIVE DATE

The ISO requests an effective date of March 6, 2020 for the IROL-CIP Cost Recovery Rules, which is 60 days from the date of this filing.

VI. ADDITIONAL SUPPORTING INFORMATION

Section 35.13 of the Commission's regulations generally requires public utilities to file certain cost and other information related to an examination of traditional cost-of-service rates.⁵⁵ However, the IROL-CIP Cost Recovery Rules are not a traditional "rate," and the ISO is not a traditional investor-owned utility. In light of these circumstances, the ISO submits the following additional information in substantial compliance with relevant provisions of Section 35.13, and request a waiver of Section 35.13 of the Commission's regulations to the extent the content or form deviates from the specific technical requirements of the regulations.

35.13(b)(1) - Materials included herewith are as follows:

- ♦ this transmittal letter;
- ♦ blacklined sections of the ISO Tariff reflecting the IROL-CIP Cost Recovery Rules;
- ♦ clean sections of the ISO Tariff reflecting IROL-CIP Cost Recovery Rules;
- ♦ the Lowell Testimony;
- ♦ the LaForest Testimony;
- ♦ the Rayo Testimony; and
- ♦ a list of the governors, utility regulatory agencies in Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island and Vermont, and other entities, to which a copy of this filing has been sent.

35.13(b)(2) - The ISO requests that the IROL-CIP Cost Recovery Rules become effective on March 6, 2020.

35.13(b)(3) - Pursuant to Section 17.11(e) of the Participants Agreement, Governance Participants are being served electronically rather than by paper copy. The names and addresses of the Governance Participants are posted on the ISO's website at <https://www.iso-ne.com/participate/participant-asset-listings/directory?id=1&type=committee>. A copy of this transmittal letter and the accompanying materials have also been sent to the governors and electric utility regulatory agencies for the six New England states that comprise the New England

⁵⁵ 18 C.F.R. § 35.13 (2019).

Control Area, the New England Conference of Public Utility Commissioners, Inc., and to the New England States Committee on Electricity. Their names and addresses are shown in the attached listing. In accordance with Commission rules and practice, there is no need for the Governance Participants or the entities identified in the listing to be included on the Commission's official service list in the captioned proceeding unless such entities become intervenors in this proceeding.

35.13(b)(4) - A description of the materials submitted pursuant to this filing is contained in Section VI of this transmittal letter.

35.13(b)(5) - The reasons for this filing are discussed in this transmittal letter and in the supporting testimonies of Mr. Lowell, Mr. LaForest, and Ms. Rayo.

35.13(b)(6) - As noted in Section IV of this transmittal letter, the IROL-CIP Cost Recovery Rules reflect the outcome of the Participant Processes required by the NEPOOL Participants Agreement.

35.13(b)(7) - The ISO has no knowledge of any relevant expenses or costs of service that have been alleged or judged in any administrative or judicial proceeding to be illegal, duplicative, or unnecessary costs that are demonstrably the product of discriminatory employment practices.

VII. CONCLUSION

For the reasons stated herein, the ISO respectfully requests that the Commission accept the IROL-CIP Cost Recovery Rules as filed, without condition, suspension, or hearing, to be effective March 6, 2020.

Respectfully submitted,

By: Monica Gonzalez
Monica Gonzalez, Esq.
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040-2841
(413) 535-4178

Counsel for ISO New England Inc.

SCHEDULE 17

{RESERVED}

RECOVERY OF CRITICAL INFRASTRUCTURE PROTECTION COSTS BY FACILITIES CRITICAL TO THE DERIVATION OF INTERCONNECTION RELIABILITY OPERATING LIMITS

Introduction

NERC Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization (“CIP-002-5.1”) requires the identification, assessment and categorization of facilities that NERC defines as Bulk Electric System (“BES”) Cyber Systems and associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that their loss, compromise, or misuse could have on the reliable operation of the BES. Criterion 2.6 in Attachment 1 – Impact Rating Criteria to CIP-002-5.1 assigns a medium impact rating to generation and transmission facilities that the ISO identifies as critical to the derivation of Interconnection Reliability Operating Limits and their associated contingencies (“IROL-Critical Facilities”). In accordance with CIP-002-5.1, an owner of an IROL-Critical Facility (“IROL-Critical Facility Owner”) must comply with the controls included in the NERC CIP Reliability Standards corresponding to the medium impact category.

This Schedule 17 provides for the recovery of an IROL-Critical Facility Owner’s incremental capital, operation and maintenance, and associated administrative and regulatory costs paid to comply with the NERC CIP Reliability Standards corresponding to the medium impact category (collectively, “IROL-CIP Costs”), as approved by the Commission’s acceptance of the IROL-Critical Facility Owner’s filing pursuant to Section 205 of the Federal Power Act, at one or more IROL-Critical Facilities to the extent cost recovery for the IROL-CIP Costs is not provided for under another provision of the Tariff or a contractual arrangement to which the IROL-Critical Facility Owner is a party. Eligible IROL-CIP Costs are above and beyond the costs paid by the IROL-Critical Facility Owner to comply with NERC CIP Reliability Standards corresponding to low impact requirements. Nothing in this Schedule 17 shall restrict or limit the rights of an IROL-Critical Facility Owner to make a filing with the Commission pursuant to Section 205 of the Federal Power Act to recover IROL-CIP Costs through a means other than this Schedule 17.

Under this Schedule 17, the ISO will act as the billing and collection agent on behalf of the IROL-Critical Facility Owners for recovery of their Commission-approved IROL-CIP Costs. The ISO will allocate to, invoice, and collect from Transmission Customers that receive Regional Network Service and/or Through

or Out Service IROL-CIP Costs approved by the Commission and, upon collection of such costs, will pay equivalent amounts to the pertinent IROL-Critical Facility Owner(s), in the manner specified in this Schedule 17.

1. IROL-Critical Facility Designation and Notification

The ISO shall designate a generation facility or transmission facility as an IROL-Critical Facility in accordance with applicable NERC Reliability Standards. When the ISO identifies a generator or transmission facility as IROL-Critical, the ISO shall provide written notification of the designation to the IROL-Critical Facility Owner or its Lead Market Participant, as applicable. The notice shall specify: (a) the facility by name and asset identification if applicable, and (b) the effective date for the IROL-Critical Facility designation.

The ISO reviews IROL-Critical Facility designations annually or more frequently based on New England Transmission System changes. If, based on this review, the ISO determines that an IROL-Critical Facility no longer meets applicable NERC criteria for designation as an IROL-Critical Facility, the ISO shall provide written notice to the IROL-Critical Facility Owner or its Lead Market Participant, as applicable, of the effective date of such termination.

2. Requirements for Recovery of IROL-CIP Costs

2.1 Pre-Filing Obligations of an IROL-Critical Facility Owner

To recover IROL-CIP Costs under this Schedule 17, in accordance with Section 2.2 below, an IROL-Critical Facility Owner must submit a filing to the Commission pursuant to Section 205 of the Federal Power Act requesting approval of IROL-CIP Costs proposed to be recovered. An IROL-Critical Facility Owner that intends to make a Section 205 filing for the recovery of IROL-CIP Costs pursuant to this Schedule 17 shall comply with the following pre-filing requirements:

(A) Prior to submitting a Section 205 filing for recovery of IROL-CIP Costs, the IROL-Critical Facility Owner shall provide to the ISO a summary description of the proposed filing, including the incremental medium impact IROL-CIP Costs and the supporting data, calculations, and workpapers for those costs, with any confidential or proprietary information redacted, and contact information for the IROL-Critical Facility Owner. The ISO shall post on its website all materials provided to the ISO by the

IROL-Critical Facility Owner. To receive automated notification of the ISO's postings of the materials provided by the IROL-Critical Facility Owner, entities may self-subscribe to the ISO's Schedule 17 distribution list. Any entity that wishes to participate as an interested party ("Interested Party") in the pre-filing review process described in Sections 2.1(B) and (C) below shall contact the IROL-Critical Facility Owner to request Interested Party status by no later than the tenth day following the interactive session described in Section 2.1(B) below.

(B) No sooner than fifteen (15) days following the ISO's posting of the materials provided by the IROL-Critical Facility Owner on the ISO website, the IROL-Critical Facility Owner shall host, either in-person or on-line, an interactive briefing session to review the summary materials and examine the IROL-CIP Costs proposed for recovery.

(C) Following the interactive briefing session described in Section 2.1(B) above, the IROL-Critical Facility Owner shall provide an additional sixty (60) days for: (i) Interested Parties to raise issues and/or request further information from the IROL-Critical Facility Owner, and (ii) the IROL-Critical Facility Owner to provide the requested information and seek to address any issues presented by Interested Parties. An IROL-Critical Facility Owner may extend the 60-day period at its discretion. The IROL-Critical Facility Owner shall be free to submit its Section 205 filing for recovery of IROL-CIP Costs under this Schedule 17 no sooner than the earlier of: (i) the conclusion of the 60-day period, (ii) the eleventh day following the interactive briefing session described in Section 2.1(B) above, if no entity contacted the IROL-Critical Facility Owner seeking to participate in the pre-filing review process as an Interested Party, or (iii) the date by which all Interested Parties, as identified by the tenth day following the interactive session in accordance with Section 2.1(A) above, have informed the IROL-Critical Facility Owner that they no longer desire additional pre-filing time to review the IROL-Critical Facility Owner's IROL-CIP Cost information. The IROL-Critical Facility Owner shall provide notice of its Section 205 filing to Interested Parties.

2.2 IROL-Critical Facility Owner's Section 205 Rate Filing

(A) IROL-CIP Costs, including capital, operation and maintenance, and associated administrative and regulatory costs, are recoverable only to the extent they (i) are incurred by the IROL-Critical Facility Owner during the period in which the subject facility is designated as an IROL-Critical Facility; (ii) are paid by the IROL-Critical Facility Owner during the cost recovery period specified by the IROL-Critical Facility Owner in the Table 1 provided in Attachment to this Schedule 17; (iii) are presented by the IROL-Critical Facility Owner in a Section 205 filing and approved by the Commission; and (iv) satisfy all other conditions for recovery, as set forth in this Schedule 17. It is the responsibility

of the IROL-Critical Facility Owner to notify the ISO of the Commission's approval of its filings to recover IROL-CIP Costs under this Schedule 17.

(B) Information supporting IROL-CIP Costs proposed for recovery under this Schedule 17 shall conform to the data requirements set forth in the Table 1 provided in Attachment A to this Schedule 17, including identification of the specific IROL-Critical Facility associated with the claimed IROL-CIP Costs; categorization of costs by function and subject matter; and specification of the cost recovery period in which the costs were paid. The IROL-Critical Facility Owner bears all responsibility for supporting claimed IROL-CIP Costs, for satisfying the requirements of Section 205, and for demonstrating eligibility for recovery under this Schedule 17.

(C) An IROL-Critical Facility Owner may submit a Section 205 filing to recover IROL-CIP Costs under this Schedule 17 no more frequently than once every twelve (12) months. However, the time-period for which IROL-CIP Costs are claimed (and reflected in such Section 205 filings) is not limited to twelve (12) months.

3. Invoicing and Collection of IROL-CIP Costs by ISO

The ISO acts as the billing and collection agent on behalf of the IROL-Critical Facility Owner for recovery of IROL-CIP Costs approved by the Commission's acceptance of the IROL-Critical Facility Owner's filing pursuant to Section 205 of the Federal Power Act. Upon notification from the IROL-Critical Facility Owner that a Commission Order approving IROL-CIP Costs for recovery under this Schedule 17 has been issued, the ISO shall initiate payment of such costs to the IROL-Critical Facility Owners, and allocation and invoicing of such costs to Transmission Customers in the manner set forth in Sections 3.1 and 3.2 below.

3.1 Monthly Payment to IROL-Critical Facility Owner

The ISO shall remit Commission-approved IROL-CIP Costs collected by the ISO in monthly payments of equal amounts over twelve (12) consecutive months to the applicable Market Participants based on their respective ownership shares in an associated IROL-Critical Facility. The ISO shall commence monthly payment of IROL-CIP Costs in the Monthly Statement issued for the first month immediately following the ISO's receipt of the IROL-Critical Facility Owner's notification of the Commission Order approving IROL-CIP Costs for recovery.

3.2 IROL-CIP Charges

The ISO shall invoice the total of Commission-approved IROL-CIP Cost in a given month to Transmission Customers receiving Regional Network Service or Through or Out Service on a monthly basis. Each Transmission Customer shall pay a charge for IROL-CIP Costs (“IROL-CIP Charge”) in each month, which charge shall be calculated using the following formula:

$$\underline{IROL-CIP\ Charge_{month}} = CIP_{month} \times \frac{[MRNL_{month,c} + AVETOUT_{month,c}]}{[\sum_{c=1}^{customers} MRNL_{month,c} + \sum_{c=1}^{customers} AVETOUT_{month,c}]}$$

Where:

CIP_{month} = Total IROL-CIP Costs_m payments made to IROL-Critical Facility Owners in month m.

$MRNL_{month,c}$ = Regional Network Load in the month for customer c

$AVETOUT_{month,c}$ = Average across the hours in the month of Reserved Capacity for Through or Out Service (excluding any Coordinated External Transaction Reserved Capacity for Through or Out Service) for customer c

ATTACHMENT A TO SCHEDULE 17

Table 1 - Incremental CIP Compliance Costs for a Facility Designated as IROL-Critical
Required Information

General Information

Facility Name	
Asset ID	
Date of IROL-Critical Designation (mm/yyyy)	
Summer Claimed Capability (MW)	
Winter Claimed Capability (MW)	
Original In-Service Date	
Interconnection Voltage	
Primary Fuel	
Dual Fuel Capable? (y/n)	
Facility includes External Routable Connectivity (y/n)	
Part of a Multi-unit Station? (y/n)	
If yes, number of units at the station	

Cost Recovery Period during which CIP Costs were Paid

Starting Date of Cost Recovery Period	
Ending Date of Cost Recovery Period	

Actual Paid Incremental Costs for the Specified Period

	Total Incremental CIP Compliance Costs for IROL- Critical Facility
Labor	\$ -
Equipment & Hardware	\$ -
Software/Application Licenses, Maintenance and Support, and Upgrade Costs	\$ -
Outside Services and Fees	\$ -
Physical Improvements	\$ -
Production, Printing, and Shipping Costs	\$ -
Other, including Associated Administrative and Regulatory Costs	\$ -
Total Actual Paid Incremental Costs for the Specified Period	\$ -

SCHEDULE 17
RECOVERY OF CRITICAL INFRASTRUCTURE PROTECTION COSTS
BY FACILITIES CRITICAL TO THE DERIVATION OF INTERCONNECTION RELIABILITY
OPERATING LIMITS

Introduction

NERC Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization (“CIP-002-5.1”) requires the identification, assessment and categorization of facilities that NERC defines as Bulk Electric System (“BES”) Cyber Systems and associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that their loss, compromise, or misuse could have on the reliable operation of the BES. Criterion 2.6 in Attachment 1 – Impact Rating Criteria to CIP-002-5.1 assigns a medium impact rating to generation and transmission facilities that the ISO identifies as critical to the derivation of Interconnection Reliability Operating Limits and their associated contingencies (“IROL-Critical Facilities”). In accordance with CIP-002-5.1, an owner of an IROL-Critical Facility (“IROL-Critical Facility Owner”) must comply with the controls included in the NERC CIP Reliability Standards corresponding to the medium impact category.

This Schedule 17 provides for the recovery of an IROL-Critical Facility Owner’s incremental capital, operation and maintenance, and associated administrative and regulatory costs paid to comply with the NERC CIP Reliability Standards corresponding to the medium impact category (collectively, “IROL-CIP Costs”), as approved by the Commission’s acceptance of the IROL-Critical Facility Owner’s filing pursuant to Section 205 of the Federal Power Act, at one or more IROL-Critical Facilities to the extent cost recovery for the IROL-CIP Costs is not provided for under another provision of the Tariff or a contractual arrangement to which the IROL-Critical Facility Owner is a party. Eligible IROL-CIP Costs are above and beyond the costs paid by the IROL-Critical Facility Owner to comply with NERC CIP Reliability Standards corresponding to low impact requirements. Nothing in this Schedule 17 shall restrict or limit the rights of an IROL-Critical Facility Owner to make a filing with the Commission pursuant to Section 205 of the Federal Power Act to recover IROL-CIP Costs through a means other than this Schedule 17.

Under this Schedule 17, the ISO will act as the billing and collection agent on behalf of the IROL-Critical Facility Owners for recovery of their Commission-approved IROL-CIP Costs. The ISO will allocate to, invoice, and collect from Transmission Customers that receive Regional Network Service and/or Through or Out Service IROL-CIP Costs approved by the Commission and, upon collection of such costs, will pay

equivalent amounts to the pertinent IROL-Critical Facility Owner(s), in the manner specified in this Schedule 17.

1. IROL-Critical Facility Designation and Notification

The ISO shall designate a generation facility or transmission facility as an IROL-Critical Facility in accordance with applicable NERC Reliability Standards. When the ISO identifies a generator or transmission facility as IROL-Critical, the ISO shall provide written notification of the designation to the IROL-Critical Facility Owner or its Lead Market Participant, as applicable. The notice shall specify: (a) the facility by name and asset identification if applicable, and (b) the effective date for the IROL-Critical Facility designation.

The ISO reviews IROL-Critical Facility designations annually or more frequently based on New England Transmission System changes. If, based on this review, the ISO determines that an IROL-Critical Facility no longer meets applicable NERC criteria for designation as an IROL-Critical Facility, the ISO shall provide written notice to the IROL-Critical Facility Owner or its Lead Market Participant, as applicable, of the effective date of such termination.

2. Requirements for Recovery of IROL-CIP Costs

2.1 Pre-Filing Obligations of an IROL-Critical Facility Owner

To recover IROL-CIP Costs under this Schedule 17, in accordance with Section 2.2 below, an IROL-Critical Facility Owner must submit a filing to the Commission pursuant to Section 205 of the Federal Power Act requesting approval of IROL-CIP Costs proposed to be recovered. An IROL-Critical Facility Owner that intends to make a Section 205 filing for the recovery of IROL-CIP Costs pursuant to this Schedule 17 shall comply with the following pre-filing requirements:

(A) Prior to submitting a Section 205 filing for recovery of IROL-CIP Costs, the IROL-Critical Facility Owner shall provide to the ISO a summary description of the proposed filing, including the incremental medium impact IROL-CIP Costs and the supporting data, calculations, and workpapers for those costs, with any confidential or proprietary information redacted, and contact information for the IROL-Critical Facility Owner. The ISO shall post on its website all materials provided to the ISO by the IROL-Critical Facility Owner. To receive automated notification of the ISO's postings of the materials

provided by the IROL-Critical Facility Owner, entities may self-subscribe to the ISO's Schedule 17 distribution list. Any entity that wishes to participate as an interested party ("Interested Party") in the pre-filing review process described in Sections 2.1(B) and (C) below shall contact the IROL-Critical Facility Owner to request Interested Party status by no later than the tenth day following the interactive session described in Section 2.1(B) below.

(B) No sooner than fifteen (15) days following the ISO's posting of the materials provided by the IROL-Critical Facility Owner on the ISO website, the IROL-Critical Facility Owner shall host, either in-person or on-line, an interactive briefing session to review the summary materials and examine the IROL-CIP Costs proposed for recovery.

(C) Following the interactive briefing session described in Section 2.1(B) above, the IROL-Critical Facility Owner shall provide an additional sixty (60) days for: (i) Interested Parties to raise issues and/or request further information from the IROL-Critical Facility Owner, and (ii) the IROL-Critical Facility Owner to provide the requested information and seek to address any issues presented by Interested Parties. An IROL-Critical Facility Owner may extend the 60-day period at its discretion. The IROL-Critical Facility Owner shall be free to submit its Section 205 filing for recovery of IROL-CIP Costs under this Schedule 17 no sooner than the earlier of: (i) the conclusion of the 60-day period, (ii) the eleventh day following the interactive briefing session described in Section 2.1(B) above, if no entity contacted the IROL-Critical Facility Owner seeking to participate in the pre-filing review process as an Interested Party, or (iii) the date by which all Interested Parties, as identified by the tenth day following the interactive session in accordance with Section 2.1(A) above, have informed the IROL-Critical Facility Owner that they no longer desire additional pre-filing time to review the IROL-Critical Facility Owner's IROL-CIP Cost information. The IROL-Critical Facility Owner shall provide notice of its Section 205 filing to Interested Parties.

2.2 IROL-Critical Facility Owner's Section 205 Rate Filing

(A) IROL-CIP Costs, including capital, operation and maintenance, and associated administrative and regulatory costs, are recoverable only to the extent they (i) are incurred by the IROL-Critical Facility Owner during the period in which the subject facility is designated as an IROL-Critical Facility; (ii) are paid by the IROL-Critical Facility Owner during the cost recovery period specified by the IROL-Critical Facility Owner in the Table 1 provided in Attachment to this Schedule 17; (iii) are presented by the IROL-Critical Facility Owner in a Section 205 filing and approved by the Commission; and (iv) satisfy all other conditions for recovery, as set forth in this Schedule 17. It is the responsibility

of the IROL-Critical Facility Owner to notify the ISO of the Commission's approval of its filings to recover IROL-CIP Costs under this Schedule 17.

(B) Information supporting IROL-CIP Costs proposed for recovery under this Schedule 17 shall conform to the data requirements set forth in the Table 1 provided in Attachment A to this Schedule 17, including identification of the specific IROL-Critical Facility associated with the claimed IROL-CIP Costs; categorization of costs by function and subject matter; and specification of the cost recovery period in which the costs were paid. The IROL-Critical Facility Owner bears all responsibility for supporting claimed IROL-CIP Costs, for satisfying the requirements of Section 205, and for demonstrating eligibility for recovery under this Schedule 17.

(C) An IROL-Critical Facility Owner may submit a Section 205 filing to recover IROL-CIP Costs under this Schedule 17 no more frequently than once every twelve (12) months. However, the time-period for which IROL-CIP Costs are claimed (and reflected in such Section 205 filings) is not limited to twelve (12) months.

3. Invoicing and Collection of IROL-CIP Costs by ISO

The ISO acts as the billing and collection agent on behalf of the IROL-Critical Facility Owner for recovery of IROL-CIP Costs approved by the Commission's acceptance of the IROL-Critical Facility Owner's filing pursuant to Section 205 of the Federal Power Act. Upon notification from the IROL-Critical Facility Owner that a Commission Order approving IROL-CIP Costs for recovery under this Schedule 17 has been issued, the ISO shall initiate payment of such costs to the IROL-Critical Facility Owners, and allocation and invoicing of such costs to Transmission Customers in the manner set forth in Sections 3.1 and 3.2 below.

3.1 Monthly Payment to IROL-Critical Facility Owner

The ISO shall remit Commission-approved IROL-CIP Costs collected by the ISO in monthly payments of equal amounts over twelve (12) consecutive months to the applicable Market Participants based on their respective ownership shares in an associated IROL-Critical Facility. The ISO shall commence monthly payment of IROL-CIP Costs in the Monthly Statement issued for the first month immediately following the ISO's receipt of the IROL-Critical Facility Owner's notification of the Commission Order approving IROL-CIP Costs for recovery.

3.2 IROL-CIP Charges

The ISO shall invoice the total of Commission-approved IROL-CIP Cost in a given month to Transmission Customers receiving Regional Network Service or Through or Out Service on a monthly basis. Each Transmission Customer shall pay a charge for IROL-CIP Costs (“IROL-CIP Charge”) in each month, which charge shall be calculated using the following formula:

$$IROL-CIP\ Charge_{month} = CIP_{month} \times \frac{[MRNL_{month,c} + AVETOUT_{month,c}]}{[\sum_{c=1}^{customers} MRNL_{month,c} + \sum_{c=1}^{customers} AVETOUT_{month,c}]}$$

Where:

CIP_{month} = Total IROL-CIP Costs_m payments made to IROL-Critical Facility Owners in month *m*.

$MRNL_{month,c}$ = Regional Network Load in the month for customer *c*

$AVETOUT_{month,c}$ = Average across the hours in the month of Reserved Capacity for Through or Out Service (excluding any Coordinated External Transaction Reserved Capacity for Through or Out Service) for customer *c*

ATTACHMENT A TO SCHEDULE 17

Table 1 - Incremental CIP Compliance Costs for a Facility Designated as IROL-Critical
Required Information

General Information

Facility Name	
Asset ID	
Date of IROL-Critical Designation (mm/yyyy)	
Summer Claimed Capability (MW)	
Winter Claimed Capability (MW)	
Original In-Service Date	
Interconnection Voltage	
Primary Fuel	
Dual Fuel Capable? (y/n)	
Facility includes External Routable Connectivity (y/n)	
Part of a Multi-unit Station? (y/n)	
If yes, number of units at the station	

Cost Recovery Period during which CIP Costs were Paid

Starting Date of Cost Recovery Period	
Ending Date of Cost Recovery Period	

Actual Paid Incremental Costs for the Specified Period

	Total Incremental CIP Compliance Costs for IROL- Critical Facility
Labor	\$ -
Equipment & Hardware	\$ -
Software/Application Licenses, Maintenance and Support, and Upgrade Costs	\$ -
Outside Services and Fees	\$ -
Physical Improvements	\$ -
Production, Printing, and Shipping Costs	\$ -
Other, including Associated Administrative and Regulatory Costs	\$ -
Total Actual Paid Incremental Costs for the Specified Period	\$ -

1 UNITED STATES OF AMERICA
2 BEFORE THE
3 FEDERAL ENERGY REGULATORY COMMISSION
4
5

6 ISO New England Inc. and) Docket No. ER20-____-000
7
8

9 TESTIMONY OF JONATHAN B. LOWELL
10 ON BEHALF OF ISO NEW ENGLAND INC.
11

12 I. INTRODUCTION

13 Q: PLEASE STATE YOUR NAME, POSITION, AND BUSINESS ADDRESS.

14 A: My name is Jonathan B. Lowell. I am employed by ISO New England Inc. (the
15 “ISO”), where I am a Principal Analyst in the Market Development Department.
16 My business address is One Sullivan Road, Holyoke, Massachusetts 01040.
17

18 Q: PLEASE DESCRIBE YOUR EDUCATIONAL BACKGROUND AND
19 RELEVANT PROFESSIONAL EXPERIENCE.

20 A: I am currently a Principal Analyst in the Market Development Department at the
21 ISO, where I have been employed since January 2006, with responsibilities for
22 identifying design improvements in New England’s electricity markets, and
23 drafting appropriate market rules and manuals to implement those improvements.
24 Prior to joining the ISO, I had wide-ranging experience in the electricity industry,
25 including four years with TransEnergie US, an independent transmission
26 development firm; three years in the energy practice at the economics consulting
27 firm PHB Hagler Bailly where I specialized in the economic analysis of
28 investment opportunities in competitive electricity markets; and 18 years with the

1 New England Electric System with responsibilities for resource planning and
2 portfolio management.

3 I hold a Bachelor of Science degree in Applied Mathematics from Brown
4 University and an MBA from Worcester Polytechnic Institute.

5 **II. PURPOSE AND SCOPE OF TESTIMONY**

6 **Q: WHAT IS THE PURPOSE OF YOUR TESTIMONY?**

7 A: The purpose of my testimony is to describe and support a proposed addition to
8 Section II of the ISO New England Open Access Transmission Tariff (“OATT”).
9 The addition will be a new Schedule 17, which will create a mechanism through
10 which certain generators and transmission facilities can be compensated for their
11 incremental costs to comply with the North American Electric Reliability
12 Corporation (“NERC”) critical infrastructure protection (“CIP”) standards and
13 requirements applicable to facilities that fall within the “medium impact” criteria
14 of those standards. These facilities are subject to the medium impact criteria
15 because the ISO designated them as critical to the derivation of Interconnection
16 Reliability Operating Limits (“IROL”). I will explain each of the following in
17 greater detail:

- 18 • The reliability-related costs to facilities assigned as NERC CIP medium
19 impact assets as a result of the ISO’s designation of the facilities as critical to
20 the derivation of IROLs (“IROL-Critical Facilities”), and why such costs
21 should be eligible for recovery outside the ISO-administered markets;

- 1 • The need for a cost recovery mechanism (the “IROL-CIP Cost Recovery
2 Mechanism”) in the OATT to facilitate IROL-Critical Facilities’ recovery of
3 IROL-CIP compliance costs (“IROL-CIP Costs”);
- 4 • A description of the proposed IROL-CIP Cost Recovery Mechanism,
5 including:
 - 6 ○ The filing requirements under Section 205 of the Federal Power Act
7 (“FPA”) for owners of IROL-Critical Facilities (“IROL-Critical
8 Facility Owners”), and the need for Commission acceptance of IROL-
9 CIP Costs;
 - 10 ○ Eligible IROL-CIP Costs, and why those costs are limited to actual
11 costs during the period a facility is designated by the ISO as an IROL-
12 Critical Facility, rather than forward or projected costs;
 - 13 ○ Payments and charges of IROL-CIP Costs; and
- 14 • The proposed cost allocation methodology for IROL-CIP Costs

15 The focus of my testimony is on the design of the IROL-CIP Cost Recovery
16 Mechanism. Mr. Dean LaForest of the ISO is providing testimony on how and
17 why the ISO designates certain facilities as IROL-Critical Facilities, and the
18 reliability benefit that results. Ms. Ingrid Rayo of the Burns & McDonnell
19 consulting firm is providing testimony supporting the type of direct costs IROL-
20 Critical Facility Owners are expected to incur to comply with the NERC CIP
21 Standards for medium impact assets.

1 **III. BACKGROUND**

2 **Q: WHAT ARE IROL-CRITICAL FACILITIES?**

3 A: IROL-Critical Facilities are generation and transmission facilities that the ISO has
4 identified as critical to deriving IROLs. IROL-Critical Facilities are required to
5 comply with the NERC CIP Reliability Standards' medium impact requirements
6 for Bulk Electric System ("BES") Cyber Systems. The ISO's process for
7 identifying and designating IROL-Critical Facilities is described in Mr.
8 LaForest's testimony.

9

10 **Q: PLEASE EXPLAIN THE EFFECT OF A "MEDIUM IMPACT" NERC CIP**
11 **STANDARD DESIGNATION ON AN IROL-CRITICAL FACILITY.**

12 A: As Mr. LaForest explains in detail, NERC CIP Standards require responsible
13 entities to identify, assess and categorize their BES Cyber Systems as low impact,
14 medium impact, or high impact based on the potential impact to the reliable
15 operation of the transmission system from their loss, compromise, or misuse.
16 Under the CIP version 5 standards approved in Order No. 791, all BES Cyber
17 Systems, at a minimum, must be categorized as low impact assets, and meet the
18 commensurate requirements. While the costs of complying with the low impact
19 requirements do not arise from or relate to any product or service under the ISO's
20 Tariff, they are recoverable through participation in the New England Markets as
21 ordinary costs of doing business.

22 The BES generation and transmission facilities that are designated as IROL-
23 Critical Facilities, however, are assigned as medium impact under the CIP version

1 5 standards. This designation requires IROL-Critical Facility Owners to comply
2 with higher reliability standards. The obligation of IROL-Critical Facility
3 Owners to comply with CIP standards corresponding to the medium impact
4 category arises from the ISO's designation, and is not within the IROL-Critical
5 Facility Owners' control. In most cases, designation as an IROL-Critical Facility
6 can lead to additional costs for such facilities, costs that are not typically incurred
7 by operators of other resources and facilities, but which relate to ensuring a more
8 reliable electric grid for all users of BES in the New England region, as Mr.
9 LaForest's testimony explains. These additional costs place IROL-Critical
10 Facility Owners at a financial disadvantage relative to the other resources with
11 which they compete in the New England Markets.

12 **III. PURPOSE OF COST RECOVERY MECHANISM**

13 **Q: PLEASE EXPLAIN THE PURPOSE OF THE IROL-CIP COST**
14 **RECOVERY MECHANISM.**

15 A: The IROL-CIP Cost Recovery Mechanism allows the ISO to act as a billing and
16 collection agent on behalf of IROL-Critical Facility Owners for Commission-
17 accepted incremental costs paid to comply with NERC CIP Standards for medium
18 impact assets. The IROL-CIP Cost Recovery Mechanism also allows the ISO to
19 charge IROL-CIP Costs to Transmission Customers receiving Regional
20 Transmission Service over a 12-month period, following the IROL-Critical
21 Facility Owner's notification of Commission acceptance of its costs.
22

1 **Q: PLEASE DESCRIBE THE TYPES OF COSTS THAT WILL BE**
2 **RECOVERABLE THROUGH THE IROL-CIP COST RECOVERY**
3 **MECHANISM.**

4 A: The IROL-CIP Cost Recovery Mechanism facilitates IROL-Critical Facility
5 Owners' recovery of previously paid costs that were incurred to meet the
6 compliance obligations associated with their designation as medium impact
7 assets. These costs are broken down in Attachment A to Schedule 17 into two
8 broad categories: (1) direct costs that are specifically related to NERC CIP
9 Standards; and (2) indirect costs that may arise from or be associated with an
10 IROL-Critical Facility Owner's compliance with the medium impact asset
11 requirements. The ISO itself does not have expertise regarding the types of direct
12 costs commonly associated with IROL-Critical Facilities' compliance with NERC
13 CIP Standards. Therefore, the ISO engaged Ms. Rayo to identify the medium
14 impact BES Cyber System requirements and the types of direct costs associated
15 with compliance with those requirements. Ms. Rayo's testimony describes in
16 greater detail the categories of costs directly related to compliance that would be
17 recoverable through the IROL-CIP Cost Recovery Mechanism. In addition to the
18 direct costs identified by Ms. Rayo, Attachment A identifies indirect costs (*e.g.*,
19 administrative and regulatory costs) associated with compliance with medium
20 impact requirements, so as not to foreclose IROL-Critical Facility Owners' ability
21 to propose them in their cost recovery proposals.

1 **Q: WHY SHOULD IROL-CIP COSTS BE RECOVERED THROUGH A NON-**
2 **MARKET MECHANISM LIKE SCHEDULE 17?**

3 A: As discussed in Ms. Rayo's testimony, IROL-Critical Facilities are subject to a
4 host of cyber-related compliance requirements to satisfy their obligations as
5 medium impact assets under the NERC CIP Standards. IROL-Critical Facility
6 Owners must comply with those requirements as a result of the ISO's designation,
7 at its sole discretion, of their facilities as IROL-Critical Facilities. In most cases,
8 the owners or operators of such facilities incur significant incremental costs to
9 achieve compliance, as compared to, for example, other identical resources or
10 facilities that are required only to meet the requirements of the low impact
11 standards. Accordingly, compliance with the NERC CIP Standards for medium
12 impact assets puts IROL-Critical Facilities, which are a limited subset of the BES
13 facilities in the ISO region, at a financial disadvantage relative to facilities that are
14 not medium impact assets. Given this disadvantage, and in response to requests
15 from stakeholder representatives of transmission and generation facilities
16 designated as IROL-Critical Facilities, the ISO determined that a tariff
17 mechanism for IROL-Critical Facilities to recover their incremental costs to
18 comply with the requirements for medium impact assets would be appropriate.

19
20 **Q: SCHEDULE 17 APPEARS TO INCLUDE SOME FEATURES SIMILAR**
21 **TO THOSE OF FORMULA RATES. IS THAT INTENDED?**

22 A: Yes. Two components of the formula rate construct have been incorporated into
23 Schedule 17: pre-filing stakeholder review, and a standardized form (Attachment

1 A to Schedule 17) for IROL-CIP Costs. As discussed below, Schedule 17
2 includes a meaningful pre-filing review process that incentivizes all interested
3 parties to discuss and iron out questions related to the IROL-Critical Facility
4 Owner's proposed IROL-CIP Costs for recovery prior to the Section 205 filing,
5 thereby avoiding, or at least minimizing, potentially protracted or expensive
6 litigation.

7 In stakeholder discussions, representatives of IROL-Critical Facilities repeatedly
8 expressed their willingness to be transparent about IROL-CIP Costs, with the
9 understanding that certain details (*e.g.*, software tools, hardware configurations)
10 that could be useful to a potential cyber-intruder would remain confidential. The
11 ISO agrees there will be a need to protect sensitive information.

12 After an IROL-Critical Facility Owner submits and receives approval of its first
13 Section 205 filing for IROL-CIP Costs, subsequent Section 205 filings should
14 become similar to formula rate informational filings. Controversial issues
15 presumably will have been resolved in the initial Section 205 filing. Supporting
16 workpapers will be updated with new information. The pre-filing review process
17 should function very much like the review protocol included in a formula rate,
18 where new issues can be discussed and resolved. If the parties are successful,
19 IROL-Critical Facility Owners' subsequent Section 205 filings should be
20 uncontested. The ISO believes the time and effort all parties invest in subsequent
21 Section 205 filings will be comparable to what would be required with a formula
22 rate.

23

1 **IV. OVERVIEW OF THE IROL-CIP COST RECOVERY MECHANISM**
2 **(SCHEDULE 17)**

3 **Q: PLEASE SUMMARIZE THE IROL-CIP COST RECOVERY**
4 **MECHANISM IN SCHEDULE 17.**

5 A: Schedule 17 is comprised of three key sections and an Attachment A. Section 1
6 discusses the ISO's process for designating IROL-Critical Facilities and notifying
7 IROL-Critical Facilities of that designation. Section 2 discusses the eligibility
8 requirements for cost recovery through Schedule 17, including the pre-filing
9 review process, and the standardized requirements and parameters for an IROL-
10 Critical Facility Owner's Section 205 filing to seek recovery of IROL-CIP Costs.
11 Section 3 outlines the ISO's authorization to charge and disburse Commission-
12 approved IROL-CIP Costs, and the manner in which these costs are allocated to
13 Transmission Customers. Finally, Attachment A lists the cost categories
14 associated with compliance with NERC CIP standards applicable to medium
15 impact assets, which is intended to help standardize individual IROL-Critical
16 Facility Owners' Section 205 filings.

17
18 **Q: PLEASE DESCRIBE THE IROL-CIP COSTS ELIGIBLE FOR**
19 **RECOVERY UNDER SCHEDULE 17.**

20 A: Schedule 17 defines IROL-CIP Costs as the "incremental capital, operation and
21 maintenance, and associated administrative and regulatory costs paid to comply
22 with the NERC CIP Reliability Standards" corresponding to the medium impact
23 assets. For purposes of this definition, "incremental costs" means the additional

1 costs paid in excess of costs that would otherwise have been incurred to meet the
2 CIP standards for low impact assets. To ensure against potential for double
3 recovery, Schedule 17 explicitly excludes costs already subject to recovery under
4 another provision of the OATT or a contractual arrangement to which the IROL-
5 Critical Facility Owner is a party.

6

7 **Q: CAN A FACILITY FILE FOR RECOVERY OF PROJECTED IROL-CIP**
8 **COSTS IMMEDIATELY UPON NOTIFICATION BY THE ISO OF**
9 **DESIGNATION AS AN IROL-CRITICAL FACILITY UNDER**
10 **SCHEDULE 17?**

11 A: No. Schedule 17 limits recovery to costs actually incurred while designated as an
12 IROL-Critical Facility. In addition, recoverable costs must have actually been
13 paid by the IROL-Critical Facility Owner, not just committed for future payment,
14 to comply with the medium impact asset obligations. This aspect of the Schedule
15 17 mechanism is intentionally more limited than the Commission's base
16 period/test period ratemaking regulations. As noted previously, the objective of
17 Schedule 17 is to provide a streamlined, less litigious option for recovery of
18 IROL-CIP Costs. The proposal achieves this by narrowing the scope of filings for
19 recovery of IROL-CIP Costs to those paid costs, thus eliminating disputes related
20 to cost projections. An IROL-Critical Facility Owner retains the option to forego
21 recovery under Schedule 17 in favor of an individual rate filing under FPA
22 Section 205, in which costs committed for future payment could be considered.

23

1 **Q: PLEASE DESCRIBE THE PRE-FILING REVIEW OBLIGATIONS IN**
2 **SCHEDULE 17, SECTION 2.1.**

3 A: The pre-filing review process provides interested parties with an opportunity to
4 review, understand, and seek clarification of an IROL-Critical Facility Owner's
5 IROL-CIP Costs. As mentioned earlier, this process is modeled on the formula
6 rate review protocol, and is designed to identify and resolve interested parties'
7 concerns prior to filing and avoid unnecessary litigation.

8 The pre-filing review process includes four key steps. First, an IROL-Critical
9 Facility Owner provides non-confidential IROL-CIP Costs, and supporting
10 documents, to the ISO. Second, the ISO posts all materials provided by the
11 IROL-Critical Facility Owner on the ISO's website. Any entity self-subscribed to
12 the ISO's IROL-CIP email distribution list will automatically receive notice of the
13 posting. Third, no sooner than 15 days after posting, the IROL-Critical Facility
14 Owner must host a briefing session, after which any entity that wishes to
15 participate in the pre-filing review process must contact the IROL-Critical Facility
16 Owner to request "Interested Party" status. Finally, the IROL-Critical Facility
17 Owner is free to submit its IROL-CIP Costs for approval pursuant to Section 205
18 of the FPA 60 days after the briefing session. However, if there are no interested
19 parties or interested parties inform the IROL-Critical Facility Owner that they no
20 longer desire additional pre-filing time, the IROL-Critical Facility Owner may
21 proceed with the filing without awaiting the end of the 60-day period.

1 **Q: PLEASE EXPLAIN THE INFORMATION REQUIREMENTS THAT**
2 **SCHEDULE 17 SPECIFIES FOR A SECTION 205 FILING.**

3 A: Schedule 17, Section 2.2 provides the requirements for individual IROL-Critical
4 Facility Owners' Section 205 filings. These requirements include general
5 information describing the IROL-Critical Facility; eligible IROL-CIP Costs,
6 which must be categorized by function and subject matter; and the cost recovery
7 period in which the costs were paid. This requirement is intended to provide a
8 standard format for such filings and the costs to be presented, which, in turn,
9 should contribute to minimizing controversy regarding such filings.

10

11 **Q: ARE THERE DEADLINES ASSOCIATED WITH SUBMISSION OF**
12 **SECTION 205 FILINGS?**

13 A: No. The timing of filings is flexible and determined by each IROL-Critical
14 Facility Owner. Schedule 17, Section 2.2(c) provides that filings may be made at
15 irregular intervals rather than annually; however, filings may not occur more
16 frequently than every 12 months. This feature is intended to avoid multiple,
17 simultaneous filings by various IROL-Critical Facility Owners and improve the
18 overall efficiency of the Schedule 17 cost recovery mechanism. IROL-Critical
19 Facility Owners have the flexibility to submit Section 205 filings less frequently
20 that include costs paid over periods of varying duration (*e.g.*, 12 months, 16
21 months, 36 months, etc.), as long as a filing does not include a cost recovery
22 period that overlaps with a previous Schedule 17 filing.

23

1 **Q: PLEASE DESCRIBE HOW PAYMENTS AND CHARGES OF IROL-CIP**
2 **COSTS ARE MADE UNDER THE IROL-CIP COST RECOVERY**
3 **MECHANISM.**

4 A: The ISO will initiate payments to an IROL-Critical Facility Owner after receiving
5 notice of the Commission's acceptance of the Schedule 17 filing. The total
6 amount of accepted IROL-CIP Costs is paid to the IROL-Critical Facility Owner
7 in 12 equal monthly payments. This approach is designed to avoid "rate shock"
8 to Transmission Customers that could result from a single lump sum payment
9 while not unduly delaying compensation to an IROL-Critical Facility Owner.
10 Total monthly payments to IROL-Critical Facility Owners will be charged to
11 Transmission Customers receiving Regional Network Service or Through or Out
12 Service over a 12-month period. Each customer's pro rata share of the IROL-CIP
13 Costs is based on the customer's monthly Regional Network Load, or the average
14 monthly Through or Out Service reservation.

15 **V. COST ALLOCATION**

16 **Q: HOW DOES THE ISO PROPOSE TO ALLOCATE IROL-CIP COSTS?**

17 A: The ISO proposes to allocate IROL-CIP Costs to all Regional Transmission
18 Customers. As discussed below, these costs are incurred to ensure the secure and
19 reliable operation of the New England Transmission System and therefore should
20 be allocated to users of the transmission system in a manner similar to the costs of
21 building, maintaining, and operating the transmission system. The ISO will
22 itemize IROL-CIP Costs separate from other transmission-related costs.
23

1 **Q: DOES THIS CONCLUDE YOUR TESTIMONY?**

2 A: Yes, this concludes my testimony.

3

4 I declare under penalty of perjury that the foregoing is true and correct.

5

6 Executed on January 6, 2020.

7

8

9

10



Jonathan B. Lowell

1 **UNITED STATES OF AMERICA**
2 **BEFORE THE**
3 **FEDERAL ENERGY REGULATORY COMMISSION**

4
5
6 **ISO New England Inc.** **) Docket No. ER20-____-000**

7
8 **TESTIMONY OF DEAN L. LAFOREST**
9 **ON BEHALF OF ISO NEW ENGLAND INC.**
10

11 **I. INTRODUCTION**

12 **Q: PLEASE STATE YOUR NAME, TITLE, AND BUSINESS ADDRESS.**

13 A: My name is Dean L. LaForest. I am the Manager, Real-Time Studies in System
14 Operations for ISO New England Inc. (the “ISO”).¹ My business address is One
15 Sullivan Road, Holyoke, Massachusetts 01040.

16
17 **Q: PLEASE DESCRIBE YOUR EDUCATIONAL BACKGROUND AND**
18 **RELEVANT PROFESSIONAL EXPERIENCE.**

19 A: I am currently Manager, Real-Time Studies in the ISO’s System Operations
20 Department. In this role, I am responsible for managing the System Operations’
21 engineers who provide real-time support to the ISO’s control room and outage
22 coordination, including responding to inquiries on Interconnection Reliability
23 Operating Limits (“IROL”) based on real-time conditions. My responsibilities
24 include determining which transmission and generation facilities within the New

¹ Capitalized terms used but not defined in this filing letter have meanings ascribed thereto in the ISO’s Transmission, Markets and Services Tariff (the “Tariff”). Section II of the Tariff contains the Open Access Transmission Tariff (the “OATT”).

1 England Transmission System² are critical to the derivation of IROLs (“IROL-
2 Critical Facilities”). Prior to joining the ISO, I worked for the Vermont Electric
3 Power Company (“VELCO”) for over 14 years with managerial roles in
4 transmission planning, system operations and transmission capital projects, and
5 before that as a transmission planning and operations engineer. Before joining
6 VELCO, I worked for General Electric and Electric Power Consultants, Inc. as an
7 engineer specializing in power system analysis. I have over 30 years of
8 experience working as an electrical engineer in the power industry. I earned my
9 Bachelor’s degree in Electrical Engineering from Clarkson University.

10 **II. PURPOSE AND SCOPE OF THE TESTIMONY**

11 **Q: WHAT IS THE PURPOSE OF YOUR TESTIMONY?**

12 A: The purpose of my testimony is to support the ISO’s proposal to incorporate, in a
13 new Schedule 17 of the OATT, a mechanism through which IROL-Critical
14 Facilities can be compensated for incremental costs to comply with the North
15 American Electric Reliability Corporation (“NERC”) critical infrastructure
16 protection (“CIP”) standards and requirements applicable to facilities that fall
17 within the “medium impact” criteria of those standards (“IROL-CIP Cost
18 Recovery Mechanism”).³ Specifically, my testimony addresses how and why the

² The New England Transmission System is defined in Section I.2.2 of the Tariff, and includes the Reliability Coordinator Area/Balancing Authority Area (“RCA/BAA”), Bulk Electric System (“BES”) and bulk power elements found within New England on the transmission network.

³ See *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization*, North American Reliability Corporation, <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf> (last visited January 3, 2020) (“CIP-002-5.1”).

1 ISO designates certain facilities as IROL-Critical Facilities, and the reliability
2 benefits that results. Mr. Jonathan B. Lowell, Principal Analyst in the Markets
3 Development Department for the ISO, is providing separate testimony to describe
4 and support the proposed revisions to the OATT to reflect the IROL-CIP Cost
5 Recovery Mechanism.

6 **III. DESIGNATION OF FACILITIES CRITICAL TO IROL**

7 **Q: WHAT IS AN INTERCONNECTION RELIABILITY OPERATING LIMIT?**

8 A: The ISO operates the New England Transmission System to protect against
9 adverse impacts, such as, instability, uncontrolled separation, or cascading
10 outages, from single-element and specified multiple-element contingencies (*i.e.*,
11 an unexpected failure or outage of a system component such as a generator,
12 transmission line, circuit breaker or switch or other electrical element). To that
13 end, the ISO establishes limits for the most critical system operating parameters
14 of the system which preclude, on a pre- and post-contingency basis, such adverse
15 impacts. IROLs are among the limits used for operational planning and real-time
16 operation of the New England Transmission System. As defined by NERC, an
17 IROL is “a System Operating Limit that, if violated, could lead to instability,
18 uncontrolled separation, or Cascading outages that adversely impact the reliability
19 of the Bulk Electric System.”⁴ In New England, IROLs are the subset of SOLs⁵

⁴ See Glossary of Terms Used in NERC Reliability Standards, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (last visited December 27, 2019) (“NERC Glossary of Terms”).

⁵ An SOL is a value (e.g., MW, MVAR, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating limits for a specified system configuration to operate within acceptable reliability criteria and ratings. ISO New England Operating Procedure No. 19 – Transmission Operations (“OP-19”),

1 that the ISO has identified as having an adverse impact *beyond* the New England
2 Transmission System. Examples of unacceptable system performance that may
3 result in an IROL include, but are not limited to: system instability; oscillatory or
4 negatively dampened system response; an inability to determine if a discrete
5 bounded sub-area of the system is susceptible to voltage collapse or uncontrolled
6 separation from the rest of the system; analysis results indicating the isolation of a
7 sub-area supplying more than 1,200 MW to the rest of the system, or absorbing
8 more than 1,200 MW of power from the rest of the system; or uncontrolled
9 islanding. IROLs may be identified as a contingency (*e.g.*, a large source or load
10 loss) or may be based on dynamic system phenomena such as instability or
11 voltage collapse that can significantly impact the New England Transmission
12 System and other regions.

13
14 **Q: HOW ARE IROLs ESTABLISHED OR IDENTIFIED IN NEW**
15 **ENGLAND?**

16 A: As the Reliability Coordinator for New England, the ISO is responsible for
17 identifying the subset of SOLs that qualify as IROLs. The ISO identifies IROLs
18 using the SOL methodology established in accordance with NERC Reliability
19 Standard FAC-011 – System Operating Limits Methodology for the Operations
20 Horizon. The ISO’s SOL methodology for operational planning and real-time
21 operations of the New England Transmission System is documented in the ISO’s

available at https://www.iso-ne.com/static-assets/documents/rules_proceeds/operating/isone/op19/op19_rto_final.pdf.

1 *Master/Local Control Center Procedure No. 15 (M/LCC 15) System Operating*
2 *Limits Methodology*.⁶ The SOL methodology requires that the limits provide
3 acceptable New England Transmission System performance. In other words, the
4 system has to be operated so that it demonstrates transient, dynamic and voltage
5 stability and all facilities within their limits pre- and post-contingency state. The
6 ISO performs studies to establish transmission interface limits to prevent adverse
7 impacts, such as unit/area instability, insufficiently dampened system response, or
8 unacceptable transient low voltage conditions, by testing a range of system
9 conditions and contingencies. During testing, the ISO considers significant
10 sensitivities of the limit to generator dispatch, reactive equipment availability,
11 bus/breaker configurations, line/breaker-out conditions, among others. A
12 generation or transmission facility whose failure, degradation or disconnection is
13 determined to be impactful to an IROL during testing is designated by the ISO as
14 critical to the derivation of an IROL. Such designation is at the ISO's sole
15 discretion, and may depend on a number of factors, such as system topology,
16 power transfers, the facility's location on the system, load distribution, etc. The
17 ISO, together with the local control centers in New England, continuously
18 monitor system loading and applicable elements that are, or could be, critical to
19 IROLs. This constant monitoring allows the ISO to know the current status of all
20 facilities whose failure, degradation, or disconnection could impact an IROL.

⁶ https://www.iso-ne.com/static-assets/documents/rules_proceeds/operating/mast_satllte/mlcc15.pdf.

1 **Q: HOW MANY FACILITIES ARE CURRENTLY DESIGNATED AS IROL-**
2 **CRITICAL FACILITIES?**

3 A: As of January 2020, of the 400 plus generating facilities in New England, only 15
4 stations, comprising 27 generator units are designated as IROL-Critical Facilities.
5 There are also transmission facilities, including a merchant facility, designated as
6 IROL-Critical Facilities. The number of facilities designated as IROL-Critical
7 Facilities is not static, however. The ISO reviews IROL-Critical Facility
8 designations at least annually, or more frequently if warranted by significant
9 changes on the New England Transmission System. Generation and transmission
10 facilities may become part of or create a new IROL condition based on changes to
11 the New England Transmission System, such as changes in network load,
12 topology, and generation dispatch which may alter the system's response to an
13 event. Likewise, system changes may result in the termination of a facility's
14 previous designation as an IROL-Critical Facility.

15

16 **Q: DOES THE ISO NOTIFY THE FACILITY OWNER WHEN ITS**
17 **FACILITY HAS BEEN FOUND TO BE CRITICAL TO THE**
18 **DERIVATION OF AN IROL?**

19 A: Yes. When the ISO identifies a generation or transmission facility as critical to
20 the derivation of an IROL, it provides written notification of a designation to the
21 facility owner or its associated Market Participant. Indeed, the ISO has been
22 notifying participants associated with IROL-Critical Facilities identified per the
23 applicable NERC standards since 2013 for transmission facilities and 2014 for

1 generation facilities. The ISO's notifications identify the facility designated as an
2 IROL-Critical Facility and the effective date of the designation or the date when
3 the designation terminated if the facility no longer meets the criteria.
4

5 **Q: ARE THERE IMPLICATIONS TO A FACILITY THAT THE ISO**
6 **DESIGANTES AS AN IROL-CRITICAL FACILITY?**

7 A: Yes. Under NERC Reliability Standard CIP-002-5.1, responsible entities (in this
8 case, the IROL-Critical Facility Owners) must assess, identify and categorize each
9 of their BES Cyber Systems according to specific criteria provided in the
10 Attachment 1 – Impact Rating Criteria to the standard. These standards
11 characterize the impact that the loss, compromise, or misuse of each BES Cyber
12 System could have on the reliable operation of the Bulk Electric System. Once a
13 BES Cyber System is categorized, the responsible entity must then comply with
14 the CIP standard requirements that apply to the facility's impact category.
15 Criterion 2.6 in Section 2 of the Attachment 1 assigns a medium impact rating to
16 generation and transmission facilities identified by the ISO, as the Reliability
17 Coordinator, as critical to the derivation of an IROL. Accordingly, the IROL-
18 Critical Facility Owners of the subset of generation and transmission facilities that
19 the ISO designates, at its sole discretion, as IROL-Critical Facilities must comply
20 with the CIP standards' requirements for medium impact BES Cyber Systems.
21
22

1 **Q: ARE THERE OTHER FACILITIES IN NEW ENGLAND THAT MEET**
2 **OTHER SECTION 2 CRITERIA FOR MEDIUM IMPACT?**

3 A: Yes. All BES generation and transmission facilities in the New England
4 Transmission System must comply, at minimum, with low impact rating
5 requirements. However, there are certain transmission facilities in New England
6 that meet criteria 2.3 and 2.9 in Section 2 of Attachment 1 to CIP-002-5.1. The
7 ISO's proposal, however, is focused only on facilities that meet criterion 2.6 as
8 IROL-Critical Facilities.

9

10 **Q: ARE THERE BENEFITS TO THE NEW ENGLAND TRANSMISSION**
11 **SYSTEMS FROM AN IROL-CRITICAL FACILITY'S COMPLIANCE**
12 **WITH THE CIP STANDARDS FOR MEDIUM IMPACT RATING?**

13 A: Yes. The basis for IROL-Critical Facilities' compliance with NERC CIP
14 standards' requirements for Medium Impact assets is to ensure the reliable
15 operation of the New England Transmission System. IROL-Critical Facilities'
16 compliance allows the ISO to operate the system with higher limits without
17 unacceptable reliability risks. Conversely, compromised IROL-Critical Facility
18 elements can lead to incorrectly determined IROLs. System operations based on
19 faulty limits can result in local or wide-spread system instabilities that could
20 potentially lead to uncontrolled separation, cascading outages, or blackouts in the
21 New England Transmission System and neighboring systems.

22

23

1 Q: DOES THIS CONCLUDE YOUR TESTIMONY?

2

3 A: Yes, this concludes my testimony.

4

5 I declare under penalty of perjury that the foregoing is true and correct.

6

7 Executed on January 6, 2020.

8

9

10

11


Dean L. LaForest

1 UNITED STATES OF AMERICA
2 BEFORE THE
3 FEDERAL ENERGY REGULATORY COMMISSION
4
5
6

7 ISO New England Inc. and) Docket No. ER20-____-000
8

9 TESTIMONY OF INGRID RAYO
10 ON BEHALF OF ISO NEW ENGLAND INC.
11

12 I. INTRODUCTION

13 Q: PLEASE STATE YOUR NAME, POSITION, AND BUSINESS ADDRESS.

14 A: My name is Ingrid Rayo. I am employed by Burns & McDonnell Engineering
15 (“Burns & McDonnell”), where I am a Senior Reliability Consultant with
16 responsibilities for developing, implementing, and managing cyber security
17 programs for Information Technology and Industrial Control Systems. I have
18 been engaged by ISO New England Inc. (the “ISO”) to provide expert testimony
19 on the costs involved to comply with the North American Electric Reliability
20 Corporation (“NERC”) Critical Infrastructure Protection (“CIP”) standards. My
21 business address is 9400 Ward Parkway, Kansas City, Missouri 64114.
22

23 Q: PLEASE DESCRIBE YOUR EDUCATIONAL BACKGROUND AND
24 RELEVANT PROFESSIONAL EXPERIENCE OF YOU AND YOUR
25 FIRM.

26 I am currently a Senior Reliability Consultant with Burns & McDonnell. Burns &
27 McDonnell is a major international engineering, architecture and consulting firm
28 established in 1898. Burns & McDonnell has significant experience in

1 developing and implementing security programs, both cyber and physical with a
2 focus on allocating budgets to achieve better yields in compliance investments
3 and security. Over the past fifteen years, Burns & McDonnell have supported
4 numerous Generation, Transmission and Control Centers facilities in building
5 their compliance programs often serving as an integrator with over 15,000
6 technology implementation hours which includes program and budget oversight.
7 As a result of these partnerships and intricate knowledge of their regulatory
8 programs and costs, we frequently served as expert witnesses before the various
9 Public Utility Commissions, advisors for system operators and municipals to help
10 build support for increased investments including rate case justifications and asset
11 acquisitions.

12
13 After graduating from The University of Tulsa, I began my career in Information
14 Technology as a Regional Computer Coordinator working for a New York based
15 corporation that supported the United States Environmental Protection Agency.
16 While working full time, I continued my post baccalaureate education at Southern
17 Methodist University – School of Engineering and Applied Sciences and sparked
18 an interest in Sarbanes-Oxley compliance. In 2008, I was recruited to consult and
19 support NERC Compliance for a Kentucky utility and then accepted permanent
20 positions to support utilities in Maryland and Florida. In 2012, I joined Burns &
21 McDonnell and continued to lead projects assisting dozens of utilities in the
22 continental U.S. and Canada. I hold active Global Industrial Controls System
23 Professional (GICSP), GIAC Critical Infrastructure Protection (GCIP), and Texas

1 Infrastructure Liaison Officer (Tx ILO) industry related certifications with access
2 to the Department of Homeland Security's Homeland Security Information
3 Network (HSIN). I have worked in the Information Technology arena for over
4 twenty (20) years, of which ten (10) years have been dedicated to supporting CIP
5 programs for NERC Registered Entities.

6

7 **II. PURPOSE AND SCOPE OF TESTIMONY**

8 **Q: WHAT IS THE PURPOSE OF YOUR TESTIMONY?**

9 A: The purpose of my testimony is to describe the nature of reasonable costs a
10 generator or transmission facility is likely to incur to directly comply with the
11 NERC standards and CIP requirements relevant to facilities that are classified
12 under NERC Reliability Standard CIP-002-5.1a, Criterion 2.6 as "medium
13 impact". I will explain:

- 14 • The principal activities a facility owner must undertake to meet the medium
15 impact requirements;
- 16 • The significant difference in scope between the low impact requirements and
17 the medium impact requirements;
- 18 • The various strategies different entities around the country have adopted to
19 ensure compliance, the factors that favor one strategy over another, and how
20 that in turn impacts the reasonable costs of compliance;
- 21 • The characteristics of specific facilities that influence each facility's
22 reasonable cost of compliance;
- 23 • The use of audits by NERC and regional reliability coordinators (such as

- 1 NPCC) to enforce compliance with the CIP requirements;
- 2 • The need to document actions and procedures used as evidence of
- 3 compliance; and
- 4 • The broad categories of expenditures into which reasonable compliance costs
- 5 can be summarized.

6 I have not been asked to estimate the magnitude of reasonable compliance costs,

7 as that is very dependent on facility specific factors I have touched on above, and

8 will explain in greater detail in the remainder of my testimony.

9

10 **Q: PLEASE EXPLAIN THE FUNDAMENTAL PURPOSE OF THE NERC**

11 **CIP STANDARDS AND WHY THAT IS IMPORTANT.**

12 **A:** The NERC CIP Standards were established to guide utilities in developing and

13 implementing a cyber and physical security program to protect the critical

14 electricity infrastructure of North America. The CIP Standards promote robust

15 security practices for, but are not limited to, asset management, configuration

16 management, change management, access management, network segregation,

17 physical access, incident response, recovery, supply chain management,

18 awareness and training, personnel risk assessments, information protection, and

19 vulnerability assessments.

20

21 Cyber and physical attacks on industrial control systems and critical infrastructure

22 are increasingly on the rise and becoming more targeted and advanced. The Bulk

1 Electric System¹ (“BES”) is the largest system that supports our daily life and
2 financial functions. This system is constantly increasing in complexity and
3 technical advancements, making it an ideal target for adversaries near and far.
4 The CIP Standards provide an important baseline of defense-in-depth security
5 measures that are essential to protecting properly classified cyber assets that
6 support North America’s interconnected BES.

7
8 **Q: DO ALL FACILITIES THAT ARE PART OF THE BULK ELECTRIC**
9 **SYSTEM HAVE TO MEET THE SAME REQUIREMENTS?**

10 A: Each facility tied to the BES provides a different level of service and functionality
11 to the grid. Noting the intricacies of this massive system, there is not a current
12 need to apply the same requirements to all facilities. Studies were conducted to
13 determine the criteria for categorizing facilities based on function, load, location,
14 BES reliability operating services, and impact on real-time operations within 15
15 consecutive minutes. The output of an assessment will determine whether a
16 facility and its associated cyber assets will be classified as high impact, medium
17 impact, or low impact. This classification will determine the specific
18 requirements that the facility will need to comply with for the applicable BES
19 Cyber Asset.

20

¹ On March 20, 2014, the Federal energy Regulatory Commission (“FERC”) approved the revised definition of BES, as envisioned in Order Nos. 743, 773, and 773-A. The definition includes bright-line core criteria with various enumerated inclusions and exclusions. As a result of the application of these BES definition provisions, all Elements and Facilities necessary for the reliable operation and planning of the interconnected bulk power system will be included as BES elements. BES, as defined by NERC, is all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. Additional information on inclusions and exclusions can be found at <https://www.nerc.com/pa/RAPA/BES%20DL/BES%20Definition%20Approved%20by%20FERC%203-20-14.pdf>
See NERC Bulk Electric System Definition Reference Document, Version 3, August 2018.

1 **Q: HOW DO THE REQUIREMENTS FOR MEDIUM IMPACT FACILITIES**
2 **DIFFER FROM THE REQUIREMENTS FOR LOW IMPACT**
3 **FACILITIES?**

4 A: Naturally, there are more requirements for medium impact BES Cyber Systems
5 than low impact BES Cyber Systems. In fact, CIP-003 is the only Standard
6 applicable to low impact BES Cyber Systems. The requirements for medium
7 impact BES Cyber Systems are more stringent than the requirements for low
8 impact BES Cyber Systems and are addressed in Standards CIP-004 through CIP-
9 011. Under the current enforceable NERC CIP Version 5 Standards, there are
10 nearly sixty (60) specific requirements² for medium impact BES Cyber Systems
11 with and without External Routable Connectivity, while low impact BES Cyber
12 Systems are only required to address four (4), less prescriptive, areas. Appendix
13 A of this testimony provides a summary of the NERC CIP Standards requirements
14 that are applicable to medium impact BES Cyber Systems.

15
16 **Q: WOULD YOU EXPECT THE REASONABLE COSTS OF COMPLIANCE**
17 **FOR A MEDIUM IMPACT FACILITY TO BE SIGNIFICANTLY**
18 **HIGHER THAN THOSE OF A LOW IMPACT FACILITY, AND IF SO,**
19 **WHY?**

20 A: The cost to protect medium impact BES Cyber Systems are typically significantly
21 higher than the cost associated with protecting low impact BES Cyber Systems,
22 simply by the nature of the number of additional compliance and technology

² Refer to
<https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf>

1 requirements that medium impact BES Cyber Systems are subject to. Factoring
2 in the intensity and complexity of implementing many of the medium impact BES
3 Cyber System requirements, such as, but not limited to, the need for personnel
4 background checks (CIP-004 R3), deploying and monitoring a physical access
5 control solution (CIP-006 R1), Ports & Services Tracking & Implementation
6 (CIP-007 R1), Security Patch Management (CIP-007 R2), Cyber Security
7 Incident Reporting and Response Plan Implementation and Testing (CIP-008 R2),
8 Recovery Plan Implementation and Testing (CIP-009 R2) and performing annual
9 vulnerability assessments (CIP-010 R3) inherently increases the cost of protecting
10 medium impact BES Cyber Systems versus low impact BES Cyber Systems.

11
12 **Q: SHOULD WE EXPECT ALL MEDIUM IMPACT FACILITIES TO HAVE**
13 **THE SAME OR SIMILAR COMPLIANCE COSTS, OR ARE THERE**
14 **GOOD REASONS FOR COSTS TO VARY?**

15 A: Compliance costs for each facility will vary based on the number of cyber assets
16 that are in scope, the number of resources supporting the facility, the maturity of
17 the program established, the decision to either use manual or automated processes
18 and solutions, and type of software and hardware (inclusive of customization,
19 deployment and maintenance agreements) used to support the program. In
20 general, the following types of direct cost categories should easily align across all
21 medium impact facilities, regardless of size or function:

- 22 1. Facility Staff Labor
- 23 2. Compliance Staff Labor

- 1 3. Other Labor
- 2 4. Equipment Costs
- 3 5. Software/Application Licenses, Maintenance and Support, and Upgrade
- 4 Costs
- 5 6. Outside Services and Fees
- 6 7. Physical Improvement Costs
- 7 8. Production, Printing, and Shipping Costs
- 8

9 **Q: WHAT COMPLIANCE STRATEGIES ARE WIDELY USED AROUND**
10 **THE COUNTRY?**

11 A: From the initial mandated, approved and enforceable date of Version 1 of the
12 NERC Critical Infrastructure Protection Standard in 2008 through Version 3, the
13 industry has utilized various methods; such as, the bare minimum approach, the
14 ultra conservative approach, and the more proactive strategic approach of going
15 beyond the requirements. Registered Entities were struggling with how to
16 manage the cost of developing the various NERC CIP programs and often
17 exempted many critical assets from their assessments and inventory. There was,
18 in many cases, an avoidance of acknowledging critical cyber assets and
19 developing a CIP compliance program given its heavy paperwork requirements.
20 Many utilities were not equipped or staffed appropriately to handle the additional
21 tasks to meet the evidence requirements of the standards. As the CIP standards

1 evolved from a compliance approach³ to a more risk-based approach with the
2 introduction of Version 5, many utilities started converging their programs,
3 building on existing programs which allowed for greater program maturity.
4 However, due to the risk ratings introduced in Version 5 of the CIP standards,
5 more, previously exempted, utilities became impacted resulting in many utilities
6 developing a program in less than a year.

7
8 **Q: WHAT FACTORS MIGHT CAUSE COMPLIANCE COSTS TO DIFFER**
9 **FROM ONE FACILITY TO THE NEXT?**

10 A: There are many factors that can cause the actual dollar amount of compliance to
11 differ from one facility to the next, but the categories identified earlier remain
12 relatively consistent. For example, Facility A may utilize 24/7 onsite guard
13 personnel to monitor the physical security perimeter, while Facility B opts to
14 deploy a software-based technical solution for granting and monitoring physical
15 access. In this example, Facility A, opting for a manual solution, will have higher
16 compliance costs over a long term duration compared to Facility B that opted for
17 the technical solution. Essentially, how an entity decides to achieve compliance,
18 whether through manual or automated means, can create a significant difference
19 in cost.

20

³ A “compliance approach” is focused on adherence with the NERC CIP Standards regardless to the cyber asset’s impact on the bulk power system (“BPS”), whereas a “risk-based approach” is focused on identifying, prioritizing, and addressing risks to the BPS and the entity’s operation.

1 Another factor to consider is the types of cyber assets that are being protected.

2 For example, an isolated analogue Automatic Voltage Regulator (“AVR”) may
3 require less maintenance, protection, and compliance costs compared to
4 protecting an externally accessible digital AVR.

5 Additional factors can include (1) the number of BES facilities that a utility owns
6 or operates, (2) the cost of telecommunication build-out with the increased use of
7 fiber, (3) designing to avoid single points of failure by incorporating redundant
8 systems, such as two different telecommunication providers with different Point
9 of Presence (“POP”) access, (4) building and constructing backup control rooms
10 or data centers, (5) increased cost for physical security access infrastructure such
11 as badge readers and video cameras, and (6) increased personnel cost to support
12 the expanding infrastructure.

13

14 **Q: PLEASE EXPLAIN HOW NERC MONITORS COMPLIANCE WITH CIP**
15 **STANDARDS.**

16 A: NERC monitors compliance with CIP Standards by conducting onsite audits, spot
17 checks, annual self-certifications, self-reporting by the entity, compliance
18 investigation, and complaints. Entities are required to prove compliance with
19 documented tangible evidence, which creates a need for extensive record-keeping
20 for each in-scope cyber asset as it relates to every applicable medium impact
21 requirement.

22

23

1 **Q: IS COMPLIANCE VOLUNTARY?**

2 A: Compliance with the NERC CIP Standards is not voluntary. NERC Registered
3 Entities are subject to adherence with CIP-002, at the very minimum. NERC
4 CIP-002-5.1a became effective on December 27, 2016 with the remaining CIP
5 Standards (excluding CIP-014) having an effective date of July 1, 2016, with a
6 few exceptions for phased-in requirements. IROL-Critical Facility Owners’
7 compliance with requirements associated with NERC CIP-002-5.1a is solely due
8 to ISO’s designation of the facility as an IROL-Critical Facility. It should be
9 noted that NERC’s implantation plan imposed a compliance deadline of April 1,
10 2016.

11

12 **Q: WHAT ARE THE POTENTIAL PENALTIES FOR NON-COMPLIANCE?**

13 A: Fines for non-compliance with NERC CIP requirements can reach up to one
14 million dollars (\$1,000,000) per day per violation. As of December 1, 2019,
15 NERC has assessed penalties as high as ten million dollars (\$10,000,000) to a
16 single entity with multiple violations.

17

18 **Q: GIVEN THE DIFFERENT COMPLIANCE STRATEGIES AND FACTORS**
19 **THAT MAY BE FACILITY SPECIFIC, PLEASE DESCRIBE THE**
20 **PRIMARY CATEGORIES INTO WHICH COSTS DIRECTLY RELATED**
21 **TO MEETING THE CIP REQUIREMENTS CAN BE LOGICALLY**
22 **GROUPED.**

23 A: In general, the following are logical groupings of types of direct cost categories:

1. Facility Staff Labor – Personnel employed directly by the entity to provide day-to-day operational support which includes performing routine compliance tasks such as patch and firmware updates
2. Compliance Staff Labor – Personnel employed directly by the entity to provide oversight for the compliance program, collection/review of evidence, disseminate awareness & training, and engage the FERC, NERC, and the Northeast Power Coordinating Council for New England, when necessary
3. Other Labor – Personnel employed directly by the entity that perform unscheduled one-off tasks that support the compliance program such as creating a trivia gameboard for cybersecurity awareness
4. Equipment Costs – Expenditures for tangible items such as badge readers or Cyberlocks for physical access, servers used to store BES Cyber System Information, or firewalls for network segmentation
5. Software/Application Licenses, Maintenance and Support, and Upgrade Costs – Expenditures for software that support cyber security activities such as system backups, event correlation, baseline monitoring, or malicious code detection
6. Outside Services and Fees - Personnel contracted to provide frequent services like third party vulnerability assessments, patch assessments, constant physical security monitoring, software deployments, or program development

1 7. Physical Improvement Costs - Expenditures associated with creating or
2 reinforcing physical structures such as doors or windows

3 8. Production, Printing, and Shipping Costs – Expenditures associated with
4 creating and/or disseminating information such as awareness posters or
5 printed network diagrams depicting Electronic Security Perimeters or BES
6 Cyber System Information

7
8 **Q: DO THESE CATEGORIES CORRESPOND TO THE CATEGORIES ISO**
9 **NEW ENGLAND HAS INCLUDED AS ATTACHMENT A IN THE**
10 **PROPOSED SCHEDULE 17?**

11 A: The eight (8) categories identified herein are deemed to be reasonable,
12 appropriate, and correspond to the categories that ISO New England has included
13 in the proposed Attachment A to Schedule 17 of the Open Access Transmission
14 Tariff. The standardized cost template included in Attachment A facilitates the
15 responsible entities in planning, identifying, and recording expenses incurred to
16 meet specific CIP requirements. Burns & McDonnell contends that these
17 identified and commonly observed expenditures are necessary to support a cyber
18 security program for medium impact BES Cyber Systems based on ten (10) years
19 of experience supporting Registered Entities with mandated NERC CIP
20 responsibilities.

21
22 **Q: PLEASE DISCUSS ANY EXAMPLES OF COSTS YOU HAVE**
23 **ENCOUNTERED THAT WERE UNUSUAL OR UNEXPECTED, BUT**

1 **THAT PLAYED A USEFUL ROLE AS PART OF A FACILITY’S**
2 **COMPLIANCE STRATEGY.**

3 A: Burns & McDonnell has encountered clients that required unusual and unexpected
4 expenses based on the maturity and robustness of their cyber security program
5 and internal controls. For example, Entity A implemented a strong Information
6 Protection Program which restricted electronic access to network architecture
7 diagrams with BES Cyber System Information. This restriction required
8 authorized users to request plotted versions of diagrams to be shipped with
9 tracking confirmation for delivery and returns. Over time, these printing and
10 shipping expenses amassed to a significant amount worthy of noting.

11

12 **Q: ARE THERE OTHER DIRECT COSTS YOU HAVE SEEN THAT YOU**
13 **CONSIDERED TO BE REASONABLE AND APPROPRIATE THAT DO**
14 **NOT FIT NEATLY INTO THE PRIMARY CATEGORIES YOU HAVE**
15 **IDENTIFIED?**

16 A: While the categories identified are comprehensive, reasonable, appropriate, and
17 common, there are situations that arise that may create additional expenses that do
18 not align with the eight categories identified. These costs should be funneled to
19 an “Other” category as an unforeseen catch all category bucket. An extreme
20 example of a real-life “Other” expense directly related to compliance is covering
21 the cost for near-by lodging, food, and transportation for a Cyber Security
22 Incident Response and Recovery Team during an active reportable cyber and
23 physical breach that requires onsite support outside of the personnel’s normal

1 work hours and location. These incurred costs support safety and mitigates
2 fatigue and burnout during the response and recovery process. Of course, an
3 entity seeking to be compensated for costs of an unusual nature should be
4 expected to clearly explain the need driving the expenditures and why they
5 represent an efficient solution to a particular problem.

6
7 **Q: DOES THIS CONCLUDE YOUR TESTIMONY?**

8
9 **A:** Yes, this concludes my testimony.

10
11 I declare under penalty of perjury that the foregoing is true and correct.

12
13 Executed on January 6, 2020.

14
15
16 
17 Ingrid Rayo
18
19
20

1 Appendix A: Summary of NERC CIP Medium Impact BES Cyber Systems
2

Standard	Req. #	Requirement Title	NERC CIP Requirement Detail
CIP-002-5.1a	R1	Identify in-scope facilities and Categorize in-scope systems	Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
CIP-002-5.1a	R1.2	Identify in-scope facilities and Categorize in-scope systems	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
CIP-002-5.1a	R2.1	Review and Approve Annually	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
CIP-002-5.1a	R2.2	Review and Approve Annually	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.
CIP-003-6	R1.1	High and Medium Impact BES Cyber System Cyber Security Policy elements	For its high impact and medium impact BES Cyber Systems, if any: 1. Personnel & training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BES Cyber Systems (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BES Cyber Systems (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
CIP-004-6	R1.1	High and Medium Impact BES Cyber Systems Security Awareness Program reinforcement	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.

CIP-004-6	R2.1	Cyber Security Training Content	<p>Training content on:</p> <ol style="list-style-type: none"> 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BES Cyber System Information and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 7. Recovery plans for BES Cyber Systems; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
CIP-004-6	R2.2	Cyber Security Training Pre-access Provisioning	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
CIP-004-6	R3	Personnel Risk Assessment Program	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.
CIP-004-6	R3.1	Identity Confirmation	Process to confirm identity
CIP-004-6	R3.2	Background Check	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 1. current residence, regardless of duration; and 2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.</p>
CIP-004-6	R3.3	Evaluation of Results from Background Check	Criteria or process to evaluate criminal history records checks for authorizing access
CIP-004-6	R3.4	Contractor Personnel Risk Assessment	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
CIP-004-6	R3.5	Reoccurring Personnel Risk Assessments	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
CIP-004-6	R4.1	Access Authorization	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> 1. Electronic access; 2. Unescorted physical access into a Physical Security Perimeter; and 3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6	R4.2	Quarterly Access Review	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
CIP-004-6	R4.3	Annual Privileges Review	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
CIP-004-6	R4.4	Annual BCSI Access Review	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.
CIP-004-6	R5.1	Physical and IRA Access Revocation - 24 hr. Termination	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
CIP-004-6	R5.2	Physical and Electronic Access Revocation - Business Day Role Change	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
CIP-004-6	R5.3	BCSI Revocation	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.
CIP-005-5	R1.1	Electronic Security Perimeter	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
CIP-005-5	R1.2	Electronic Security Perimeter	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
CIP-005-5	R1.3	Electronic Security Perimeter	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
CIP-005-5	R1.4	Electronic Security Perimeter	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.
CIP-005-5	R1.5	Electronic Security Perimeter	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.
CIP-005-5	R2.1	Interactive Remote Access Management	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
CIP-005-5	R2.2	Interactive Remote Access Management	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
CIP-005-5	R2.3	Interactive Remote Access Management	Require multi-factor authentication for all Interactive Remote Access sessions.

CIP-006-6	R1.1	Physical Security Plan	Define operational or procedural controls to restrict physical access.
CIP-006-6	R1.2	Physical Security Plan	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.
CIP-006-6	R1.4	Physical Security Plan	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
CIP-006-6	R1.5	Physical Security Plan	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.
CIP-006-6	R1.6	Physical Security Plan	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.
CIP-006-6	R1.7	Physical Security Plan	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.
CIP-006-6	R1.8	Physical Security Plan	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
CIP-006-6	R1.9	Physical Security Plan	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
CIP-006-6	R1.10	Physical Security Plan	<p>Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:</p> <ul style="list-style-type: none"> · encryption of data that transits such cabling and components; or · monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or · an equally effective logical protection.
CIP-006-6	R2.1	Visitor Control Program	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
CIP-006-6	R2.2	Visitor Control Program	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.
CIP-006-6	R2.3	Visitor Control Program	Retain visitor logs for at least ninety calendar days.
CIP-006-6	R3.1	Physical Access Control System Maintenance and Testing Program	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.

CIP-007-6	R1.1	Ports and Services	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.
CIP-007-6	R1.2	Ports and Services	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.
CIP-007-6	R2.1	Security Patch Management	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
CIP-007-6	R2.2	Security Patch Management	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.
CIP-007-6	R2.3	Security Patch Management	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: <ul style="list-style-type: none"> • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.
CIP-007-6	R2.4	Security Patch Management	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
CIP-007-6	R3.1	Malicious Code Prevention	Deploy method(s) to deter, detect, or prevent malicious code.
CIP-007-6	R3.2	Malicious Code Prevention	Mitigate the threat of detected malicious code.
CIP-007-6	R3.3	Malicious Code Prevention	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.
CIP-007-6	R4.1	Security Event Monitoring	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: <ol style="list-style-type: none"> 1. Detected successful login attempts; 2. Detected failed access attempts and failed login attempts; 3. Detected malicious code.
CIP-007-6	R4.2	Security Event Monitoring	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): <ol style="list-style-type: none"> 1. Detected malicious code from Part 4.1; and 2. Detected failure of Part 4.1 event logging.
CIP-007-6	R4.3	Security Event Monitoring	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.
CIP-007-6	R5.1	System Access Control	Have a method(s) to enforce authentication of interactive user access, where technically feasible.

CIP-007-6	R5.2	System Access Control	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
CIP-007-6	R5.3	System Access Control	Identify individuals who have authorized access to shared accounts.
CIP-007-6	R5.4	System Access Control	Change known default passwords, per Cyber Asset capability
CIP-007-6	R5.5	System Access Control	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.
CIP-007-6	R5.6	System Access Control	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
CIP-007-6	R5.7	System Access Control	Where technically feasible, either: <ul style="list-style-type: none"> • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.
CIP-008-5	R1.1	Cyber Security Incident Response Plan Specifications	One or more processes to identify, classify, and respond to Cyber Security Incidents.
CIP-008-5	R1.2	Cyber Security Incident Response Plan Specifications	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.
CIP-008-5	R1.3	Cyber Security Incident Response Plan Specifications	The roles and responsibilities of Cyber Security Incident response groups or individuals.
CIP-008-5	R1.4	Cyber Security Incident Response Plan Specifications	Incident handling procedures for Cyber Security Incidents.
CIP-008-5	R2.1	Cyber Security Incident Response Plan Implementation and Testing	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: <ul style="list-style-type: none"> • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.
CIP-008-5	R2.2	Cyber Security Incident Response Plan Implementation and Testing	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.

CIP-008-5	R2.3	Cyber Security Incident Response Plan Implementation and Testing	Retain records related to Reportable Cyber Security Incidents.
CIP-008-5	R3.1	Cyber Security Incident Response Plan Review, Update, and Communication	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 1. Document any lessons learned or document the absence of any lessons learned; 2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.
CIP-008-5	R3.2	Cyber Security Incident Response Plan Review, Update, and Communication	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 1. Update the Cyber Security Incident response plan(s); and 2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.
CIP-009-6	R1.1	Recovery Plan Specifications	Conditions for activation of the recovery plan(s).
CIP-009-6	R1.2	Recovery Plan Specifications	Roles and responsibilities of responders.
CIP-009-6	R1.3	Recovery Plan Specifications	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
CIP-009-6	R1.4	Recovery Plan Specifications	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.
CIP-009-6	R1.5	Recovery Plan Specifications	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.
CIP-009-6	R2.1	Recovery Plan Implementation and Testing	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.
CIP-009-6	R2.2	Recovery Plan Implementation and Testing	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.
CIP-009-6	R3.1	Recovery Plan Review, Update and Communication	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.

CIP-009-6	R3.2	Recovery Plan Review, Update and Communication	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 1. Update the recovery plan; and 2. Notify each person or group with a defined role in the recovery plan of the updates
CIP-010-2	R1.1	Configuration Change Management	Develop a baseline configuration, individually or by group, which shall include the following items: 1. Operating system(s) (including version) or firmware where no independent operating system exists; 2. Any commercially available or open-source application software (including version) intentionally installed; 3. Any custom software installed; 4. Any logical network accessible ports; and 5. Any security patches applied.
CIP-010-2	R1.2	Configuration Change Management	Authorize and document changes that deviate from the existing baseline configuration.
CIP-010-2	R1.3	Configuration Change Management	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.
CIP-010-2	R1.4	Configuration Change Management	For a change that deviates from the existing baseline configuration: 1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 3. Document the results of the verification.
CIP-010-2	R3.1	Vulnerability Assessments	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.
CIP-010-2	R3.4	Vulnerability Assessments	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.
CIP-010-2	R4	Transient Cyber Assets and Removable Media Plans	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.
CIP-011-2	R1.1	Information Protection	Method(s) to identify information that meets the definition of BES Cyber System Information.
CIP-011-2	R1.2	Information Protection	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
CIP-011-2	R2.1	BES Cyber Asset Reuse and Disposal	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.
CIP-011-2	R2.2	BES Cyber Asset Reuse and Disposal	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

New England Governors, State Utility Regulators and Related Agencies*

Connecticut

The Honorable Ned Lamont
Office of the Governor
State Capitol
210 Capitol Ave.
Hartford, CT 06106
bob.clark@ct.gov

Connecticut Attorney General Office
55 Elm Street
Hartford, CT 06106
Seth.Hollander@ct.gov
Robert.Marconi@ct.gov

Connecticut Department of Energy and
Environmental Protection
79 Elm Street
Hartford, CT 06106
steven.cadwallader@ct.gov
robert.luysterborghs@ct.gov

Connecticut Public Utilities Regulatory Authority
10 Franklin Square
New Britain, CT 06051-2605
michael.coyle@ct.gov

Maine

The Honorable Janet Mills
One State House Station
Office of the Governor
Augusta, ME 04333-0001
Jeremy.kennedy@maine.gov
Elise.baldacci@maine.gov

Maine Public Utilities Commission
18 State House Station
Augusta, ME 04333-0018
Maine.puc@maine.gov

Massachusetts

The Honorable Charles Baker
Office of the Governor
State House

Boston, MA 02133

Massachusetts Attorney General Office
One Ashburton Place
Boston, MA 02108
rebecca.tepper@state.ma.us

Massachusetts Department of Public Utilities
One South Station
Boston, MA 02110
Nancy.Stevens@state.ma.us
morgane.treanton@state.ma.us
Lindsay.griffin@mass.gov

New Hampshire

The Honorable Chris Sununu
Office of the Governor
26 Capital Street
Concord NH 03301
Jared.chicoine@nh.gov

New Hampshire Public Utilities Commission
21 South Fruit Street, Ste. 10
Concord, NH 03301-2429
tom.frantz@puc.nh.gov
george.mccluskey@puc.nh.gov
F.Ross@puc.nh.gov
David.goyette@puc.nh.gov
RegionalEnergy@puc.nh.gov
kate.bailey@puc.nh.gov
amanda.noonan@puc.nh.gov
Corrine.lemay@puc.nh.gov

Rhode Island

The Honorable Gina Raimondo
Office of the Governor
82 Smith Street
Providence, RI 02903
Rosemary.powers@governor.ri.gov
carol.grant@energy.ri.gov
christopher.kearns@energy.ri.gov
nicholas.ucci@energy.ri.gov

New England Governors, State Utility Regulators and Related Agencies*

Rhode Island Public Utilities Commission
89 Jefferson Blvd.
Warwick, RI 02888
Margaret.curran@puc.ri.gov
todd.bianco@puc.ri.gov
Marion.Gold@puc.ri.gov

Vermont

The Honorable Phil Scott
Office of the Governor
109 State Street, Pavilion
Montpelier, VT 05609
jason.gibbs@vermont.gov

Vermont Public Utility Commission
112 State Street
Montpelier, VT 05620-2701
mary-jo.krolewski@vermont.gov
sarah.hofmann@vermont.gov

Vermont Department of Public Service
112 State Street, Drawer 20
Montpelier, VT 05620-2601
bill.jordan@vermont.gov
june.tierney@vermont.gov
Ed.McNamara@vermont.gov

New England Governors, Utility Regulatory and Related Agencies

Jay Lucey
Coalition of Northeastern Governors
400 North Capitol Street, NW
Washington, DC 20001
coneg@sso.org

Heather Hunt, Executive Director
New England States Committee on Electricity
655 Longmeadow Street
Longmeadow, MA 01106
HeatherHunt@nescoe.com
JasonMarshall@nescoe.com

Meredith Hatfield, Executive Director
New England Conference of Public Utilities
Commissioners
72 N. Main Street
Concord, NH 03301
mhatfield@necpuc.org

Anthony Roisman, President
New England Conference of Public Utilities
Commissioners
112 State Street – Drawer 20
Montpelier, VT 05620
anthony.roisman@vermont.gov