UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Potential Enhancements to the Critical	)	
Infrastructure Protection Reliability	)	**Docket No. RM20-12-000**
Standards	)	

ANSWERS OF THE ISO/RTO COUNCIL

Pursuant to the Federal Energy Regulatory Commission's ("Commission") Notice of Inquiry ("NOI") issued on June 18, 2020,[1] the ISO/RTO Council ("IRC")[2] submits these comments in response to some of the questions posed by the Commission in the NOI.

In the NOI, the Commission seeks comments on certain potential enhancements to the currently-effective Critical Infrastructure Protection ("CIP") Reliability Standards. In particular, the Commission seeks comments on whether the CIP Reliability Standards adequately address the following topics: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events. In addition, the Commission seeks comments on the potential risk of a coordinated cyberattack on geographically distributed targets and whether Commission action including potential modifications to the CIP Reliability Standards would be appropriate to address such risk. The Commission poses several specific questions in the NOI. In this filing, the IRC provides its answers to those specific questions.

[1] Notice of Inquiry, *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, Docket No. RM 20-12-000 (June 18, 2020).

[2] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"), California Independent System Operator ("CAISO"), Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator of Ontario, Inc. ("IESO"), ISO New England Inc. ("ISO-NE"), Midcontinent Independent System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and Southwest Power Pool, Inc. ("SPP").

I. ANSWERS TO QUESTIONS POSED IN THE NOI

Item A1

The security controls in the Data Security Category require the management of information and records (*i.e.,* data) consistent with an organization's risk strategy to protect the confidentiality, integrity, and availability of information and data. The Commission seeks comment on whether the CIP Reliability Standards adequately address each data security subcategory as outlined in the NIST Framework and, if not, what are possible solutions, and in particular:

- Do the CIP Reliability Standards adequately address Data Security Subcategories PR.DS-4 and PR.DS-6 for medium and high impact BES Cyber Systems, and if so how?

IRC Answer

With respect to PR.DS-4 and capacity to maintain availability of information and records relevant to critical infrastructure, the CIP Reliability Standards address only access to information (CIP-004) and management of information and record handling at the end of Cyber Asset lifecycle (CIP-011, Requirement R2). The currently-effective CIP Reliability Standards do not directly address availability in terms of sources of information and records identified as relevant (BES Cyber System Information or "BCSI") to protection of critical infrastructure. The currently-effective CIP Reliability Standards adequately address this aspect of protection, with the balance of protection assumed to be provided by a responsible entity's security program that goes beyond the CIP Reliability Standard requirements, depending on risk to the organization.[3]

With respect to PR.DS-6 and mechanisms to protect integrity of software, firmware, and information, the CIP Reliability Standards do address (or will address) protection of integrity of software and firmware as referenced within CIP-010-3, Requirement R 1.6. The CIP Reliability

[3] Efforts that go beyond the CIP Reliability Standards should be acknowledged in the form of both a credit when assessing an entity's overall compliance posture and as a mitigating factor when assessing penalties.

Standards do not directly address initial and middle of lifecycle protection of integrity of information identified as relevant to protection of critical infrastructure. CIP-011 addresses handling of BCSI, including storage, security during transit, and use. CIP-011 also requires a responsible entity to develop a process to properly dispose of Cyber Assets and handle media during end of lifecycle for information stored on a Cyber Asset. Currently-effective CIP Reliability Standards address this aspect of data security adequately given the focus on availability of service and restoration of service in the present standards. Going above and beyond the currently-effective CIP Reliability Standards can be left to be addressed in the security programs of responsible entities, depending on risk.

- Do the CIP Reliability Standards adequately address the same Subcategories for low impact BES Cyber Systems, and if so how?

IRC Answer

The CIP Reliability Standards do not address concerns related to controls PR.DS-4 and PR.DS-6 with regard to low impact BES Cyber Systems. Given the roles of ISOs/RTOs, there are no low impact BES Cyber Systems in the IRC members' CIP programs. For this reason, the IRC defers to other entities with low impact BES Cyber Systems as they are in a better position to provide answers to this question than the IRC.

- If the CIP Reliability Standards do not adequately address these Subcategories, or any other Data Security Subcategories, for either low, medium or high impact BES Cyber Systems, explain whether this poses a risk to the reliable operation of the Bulk-Power System today and the Bulk-Power System of the near future.

IRC Answer

There are a number of other data security controls associated with NIST CSF (as described below). Accordingly, any security concerns would best be addressed by a responsible entity's security program that goes above and beyond the currently-effective CIP Reliability Standards, specifically, by adhering to each of the following security controls from NIST CSF:

> PR.DS-7 development and testing are kept separate from production environment – if this is not done, then development and/or testing activity or compromise of those activities may lead to adverse impact to BES Cyber Systems and the reliability functions they support.
>
> PR.DS-5 – protection against data leaks – if this is not implemented for critical infrastructure, information relevant to attacks on that infrastructure (BCSI) may fall into the hands of attackers without the defenders being aware of it, which could leave critical infrastructure more exposed than it would be had the defenders been alerted to the breach.
>
> PR.DS-3 – assets are managed formally throughout removal, transfer, and disposition. This is initially addressed by CIP-002, CIP-005, CIP-006, and CIP-010, but the processes of removal, transfer, and disposition require greater definition to ensure no opportunities arise to expose cyber assets to attack or reliability functions to failures in availability during such operations.
>
> PR.DS-2 – data in transit is protected – this receives attention in CIP-011, CIP-012 (future enforcement) and CIP-005.
>
> PR.DS-1 – data at rest is protected – this receives attention in terms of access control in CIP-004 and, for BCSI, in CIP-011. CIP-009 covers recovery of systems (including data at rest).

Item A2

The security controls in the Anomalies and Events Category require that anomalous activity is detected and the potential impact of events is understood. Furthermore, it requires that detected events are analyzed to understand attack targets and methods. The Commission seeks comment on whether the CIP Reliability Standards adequately address the detection and mitigation of anomalous activity as outlined in the NIST Framework and, if not, what are possible solutions, and in particular:

- Should low impact BES Cyber Systems be covered by Anomalies and Events Subcategories DE.AE-2 and DE.AE-4?

IRC Answer

Security programs should support all systems with controls and monitoring functions and processes applied based on risk to the organization. ISOs/RTOs have no low impact BES Cyber Systems, and leave it to other entities with such systems in their programs to answer this question.

- Do the CIP Reliability Standards adequately address Anomalies and Events Subcategories DE.AE-2 and DE.AE-4 for low impact BES Cyber Systems, and if so how?

IRC Answer

The current version of CIP-008 (Incident Reporting and Response Planning) does not apply to low impact BES Cyber Systems. However, CIP-003 does require entities to support Low Impact BES Cyber Systems with a documented incident response procedure, which should see attention in such a security program depending on risk to go above and beyond CIP Reliability Standards in terms of anomaly and event detection.

- If the CIP Reliability Standards do not adequately address these Subcategories for low impact BES Cyber Systems, explain whether this poses a risk to the reliable operation of the Bulk-Power System today and the Bulk-Power System of the near future.

IRC Answer

Security programs should support all systems with controls and monitoring functions and processes applied, based on risk to the organization. Regulation is applied to components and systems based on risk to the Bulk Power System. Risk to the Bulk Power System increases when there is a lack of support for the low-impact systems within a responsible entity’s detection and response processes. Given that CIP-003 does specify a documented incident response process for low impact BES Cyber Systems, there is some protection afforded by the CIP Reliability Standards in this regard, and entity security programs may go above and beyond the requirements of CIP Reliability Standards, depending on risk.

- If the CIP Reliability Standards do not adequately address any other Anomalies and Events Subcategories, for either low, medium or high impact BES Cyber Systems, explain whether this poses a risk to the reliable operation of the Bulk-Power System today and the Bulk-Power System of the near future.

IRC Answer

Monitoring and anomaly detection is a key component of any security program. Response processes for anomalies should address the analysis of suspected incidents and dictate responses based on risk to the organization's operation and risk tolerance. CIP-008-5 requires responsible entities to have a documented process to identify, classify, and respond to Cyber Security Incidents along with reporting requirements. CIP-003 requires a documented incident response procedure for Low impact cases, so there already is adequate coverage for these concerns in CIP Reliability Standards.

Item A3

The security controls in the Mitigation Category require that newly identified vulnerabilities are mitigated or, alternatively, documented as accepted risks. Response activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. The Commission seeks comment on whether the CIP Reliability Standards adequately address the mitigation of newly identified vulnerabilities as outlined in the NIST Framework and, if not, what are possible solutions, and in particular:

- Do the CIP Reliability Standards adequately address Mitigation Subcategories RS.MI-1 and RS.MI-2 for low, medium and high impact BES Cyber Systems, and if so how?

IRC Answer

Given the obvious nature of undertaking incident response as required in CIP-008 and CIP-003 for all cases, a robust security program adds mitigation and containment phases to a process to address incidents. The CIP Reliability Standards already require entities to formally document such a process, so additional regulation would not materially improve the situation for low, medium, or high impact BES Cyber Systems.

- Do the CIP Reliability Standards adequately address Mitigation Subcategory RS.MI-3 for low impact BES Cyber Systems, and if so how?

IRC Answer

ISOs/RTOs have no low impact BES Cyber Systems, so the IRC leaves this question to be answered by other entities with such systems in their programs.

- If the CIP Reliability Standards do not adequately address these Subcategories for low, medium or high impact BES Cyber Systems, explain whether this poses a risk to the reliable operation of the Bulk-Power System today and the Bulk-Power System of the near future.

IRC Answer

The CIP Reliability Standards address the concerns of RS.MI-1, 2, 3 adequately and do not require adjustment to lead to appropriate protections for low, medium, and high impact BES Cyber Systems.

Item B1

- Are there operating processes and procedures that can be used to evaluate, mitigate, protect against, and recover from potential geographically distributed coordinated cyberattacks? Describe generally the efficiency and effectiveness of these operating processes and procedures, including response to and recovery from a potential geographically distributed coordinated cyberattack.

IRC Answer

Power systems operations procedures deal with many forms of distributed issues and concerns (some emergencies). System restoration exercises, including NERC's biennial GridEx exercise, support the evaluation, mitigation, and recovery from cases that might result from a distributed cyberattack (and may *include scenarios that simulate the complete* loss of communications or computing resources used to operate the power system). Other system operations exercises, such as Power System Restoration exercises, are required to be conducted annually under NERC Reliability Standards EOP-005 and EOP-006. They include all system operators in the training, and refine practices between Reliability Coordinators and member (Transmission Operators and Generator Operators) entities within Reliability Coordinator footprints.

Item B2

- Are there security controls that can be used to evaluate, mitigate, and protect against potential geographically distributed coordinated cyberattacks? Describe generally the efficiency and effectiveness of these security controls in mitigating the risk of a potential geographically distributed coordinated cyberattack.

IRC Answer

DOE CRISP and the Canadian Centre for Cyber Security are existing monitoring controls that support detection of geographically distributed attacks and the involvement of E-ISAC to help coordinate a response. However, to the extent that FERC believes these are insufficient given the light distribution of CRISP subscribers and the delayed nature of information sharing and reporting, it may be worth an effort to assess (1) whether controls are sufficiently distributed geographically in order to support a requirement for response, and (2) how quickly information sharing must be accomplished to support real-time response. Present response efforts to address real-time concerns focus on each organization's practices to identify and respond to cyber security incidents.

Item B3

- Which, if any, of these processes, procedures, or security controls could enhance the currently approved CIP Reliability Standards to better address the risk of a geographically distributed coordinated cyberattack?

IRC Answer

The current GridEx exercises support present practice to identify appropriate measures to detect and respond to distributed physical and cyberattacks. The industry should continue to support such exercises and learn from them based on the complexity of the power system and the rapidly changing nature of cyberattacks.

Item B4

- What future changes to the bulk electric system design could affect the potential risks of geographically distributed coordinated cyberattacks?

IRC Answer

Distributed energy resources and other smart grid technologies (*e.g*. synchro phasors and advanced metering initiatives) have the largest potential to increase risk from geographically distributed attacks as these are inherently disbursed processes that would be more susceptible to distributed attack. Also of note, present concerns regarding cyberattacks against natural gas supply to electric grid generators should be kept in mind for distributed cyberattack drills.

Item B5

- Are current regional drill exercises and operator training effective in preparing to mitigate and recover from a geographically distributed coordinated cyberattack?

IRC Answer

GridEx and other regional exercises are intended to improve IT/Operations interaction in distributed cyber-attacks to prepare organizations to address them. These exercise help Operators improve with respect to dealing with cyberattacks and IT/Security teams need to improve with respect to catching attacks in progress and integrating response effort with systems operation teams.

- Does current initial system operator training, or refresher training, either in class or in EMS simulation, include training to recognize and respond to a coordinated cyberattack, and should that training be required?

IRC Answer

Many programs do include initial system operator training in detection and reporting of cyber events and incidents. GridEx supports refreshing that initial training with inclusion of operations teams in development of such exercises.

- Do system operators and their leadership participate, and if so, how often, in regional drills and training exercises that simulate coordinated cyberattacks on the Bulk Electric System, and should participation in such exercises be required?

IRC Answer

System operations teams frequently lead and participate in regional drills and training exercises and are usually the most enthusiastic about emergency planning. CIP-008 compliance practice already includes using artifacts from GridEx or similar exercises to meet an existing requirement. Further regulation may not be required in this case. System operations teams do not view the lack of required training specific to coordinated attacks as a gap in the NERC Reliability Standards because they practice many of these processes under existing Power System Restoration drills.

- Do system operators and their leadership participate, and if so, how often, in regional drills and training exercises that simulate coordinated cyberattacks on other critical infrastructure in addition to the bulk electric system (i.e., communication systems, pipelines, water systems, etc.), and should participation in such exercises be mandatory?

IRC Answer

As noted above, CIP-008 compliance practice already includes the use of artifacts from GridEx or similar exercises to meet an existing requirement. Accordingly, further regulation may not be required in this case.

- Discuss whether any aspects of drill exercises or operating training pertaining to mitigation and recover from a geographically distributed coordinated cyberattack should be incorporated into the Reliability Standards. In particular, while some entities may voluntarily engage in drill exercises or training, should this be required of all entities, or specific functional categories? Should participation of specific personnel categories or leadership be required?

IRC Answer

In order to retain the innovative and flexible approach that the current GridEx practice provides, entities should not be required to participate. While the leaders and staff at each organization should engage in emergency planning and training in the normal course of business and as part of their own due diligence, participation should not be mandatory because not all organizations are the same. Moreover, an express requirement may actually run counter to the innovative and flexible approach voluntary participants currently engage in with respect to their drill exercises and training because the focus could shift to simply satisfying a mandate. Current high levels of voluntary participation in drill exercises and training demonstrate the maturity of the effort across the industry as a whole, and reveal that an express requirement is not necessary. Further, as noted above, related practices already occur under existing Power System Restoration drills.

Item B6

- Describe the effectiveness of industry information sharing at mitigating potential geographically distributed coordinated cyberattacks.

IRC Answer

The industry maintains a number of different approaches to information sharing, including E-ISAC and DHS NCCIC resources. However, there are a number of innovative approaches developing to share information among ISOs/RTOs such as chat services, audio/visual collaboration tools, and other techniques explored during GridEx exercises and independently. These sorts of tools support currently-understood scenarios, and further exploration of techniques will require more involvement in development of exercises and engagement with DOE as well as other federal agencies in a position to support this sort of effective coordination.

Item B7

- Discuss whether the thresholds established in Reliability Standard CIP-002-5.1a, Attachment 1, Section 2 are appropriate to address the risk of a geographically distributed coordinated cyberattack.
- If not, what would be appropriate method or approach to identify thresholds to address the risk?
- Alternatively, what additional security controls, if implemented, would be appropriate to address the risk?

IRC Answer

Reliability Standard CIP-002-5.1a is an asset/system-based cyber security standard and, while assets are classified as high, medium, or low based on criteria, the standard does not address the topography of the grid. While thresholds in CIP-002 are not appropriate to address geographically distributed cyberattacks, they were never intended to apply to those attacks. To re-cast the CIP-002 criteria to address additional/different threats on a larger-than-organizational basis would require re-architecting the entire CIP program on the whole.

The development of a comprehensive risk-based approach to protecting the grid would require topological assessment of electrical system risk right alongside cyber security and other operational risks related to maintaining grid reliability. A more comprehensive approach to infrastructure risk management should include other sectors' influence (*e.g*., the gas/fuel and communications sectors).

II. CONCLUSION

The IRC respectfully requests that the Commission consider its answers to the questions posed by the Commission in the NOI.

Respectfully submitted,

/s/ James M. Burlew
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

/s/ Margoth Caley
Maria Gulluni
Vice President & General Counsel
Margoth Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ Anna McKenna
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
Andrew Ulmer Director, Federal Regulatory Affairs
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Carl F. Patka
Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Carl F. Patka
Assistant General Counsel
Christopher R. Sharp
Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
cpatka@nyiso.com

/s/ Andre T. Porter
Andre T. Porter
Vice President, General Counsel & Secretary
Mary-James Young
Senior Corporate Counsel
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

/s/ Paul Suskie
Paul Suskie
Executive Vice President & General Counsel
Mike Riley
Associate General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Devon Huber
Devon Huber
Senior Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto, Ontario M5H1T1
Canada
devon.huber@ieso.ca

/s/ Chad V. Seely
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
chad.seely@ercot.com

/s/ Diana Wilson
Diana Wilson
Director Enterprise Risk Management and Compliance
Alberta Electric System Operator
#2500, 330 — 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.wilson@aeso.ca

August 24, 2020