UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

POTENTIAL ENHANCEMENTS TO THE CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS	**DOCKET NO. RM20-12-000**

COMMENTS OF THE
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

The National Rural Electric Cooperative Association ("NRECA") respectfully submits comments in response to the Notice of Inquiry issued by the Federal Energy Regulatory Commission ("Commission") in this proceeding on June 18, 2020, and published in the Federal Register on June 24, 2020.[1] NRECA appreciates the Commission's efforts to understand whether the current Critical Infrastructure Protection ("CIP") Reliability Standards adequately address: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events. NRECA also understands the Commission's desire to develop a record concerning 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. NRECA requests that the Commission maintain its risk-based approach to cybersecurity of the bulk electric system ("BES") and recommends that the Commission refrain from proposing any revisions to the CIP Reliability Standards to include additional requirements for low impact assets.

---

[1] *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, 171 FERC ¶ 61,215 (2020) ("NOI").

I. DESCRIPTION OF NRECA

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landmass.[2]

Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 63 generation and transmission ("G&T") cooperatives and 834 distribution cooperatives. The G&T cooperatives generate and transmit power to distribution cooperatives that provide it to the end of line co-op consumer-members. Collectively, G&T cooperatives generate and transmit power to nearly 80 percent of the distribution cooperatives in the nation. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

NRECA's member cooperatives include Registered Entities subject to the Reliability Standards developed by the North American Electric Reliability Corporation ("NERC") and approved by the Commission pursuant to section 215 of the Federal Power Act.[3] Nearly all cooperatives, even if they are not Registered Entities, receive service from the BES and thus have an interest in the reliability of the BES. Thus, NRECA's member cooperatives have significant interests in the topics of this inquiry.

---

[2] *See* https://www.electric.coop/electric-cooperative-fact-sheet/.

[3] 16 U.S.C. § 824o (2018).

II. COMMUNICATIONS

Please direct communications concerning this pleading to the following persons and place their names on the Commission's official service list.

Barry R. Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5781
Email: barry.lawson@nreca.coop

Jesse Halpern
Thompson Coburn LLP
1909 K Street, N.W.
Suite 600
Washington, DC 20006
Telephone: (202) 585-6900
Email: jhalpern@thompsoncoburn.com

III. COMMENTS

NRECA understands the Commission's effort to consider potential enhancements to the CIP Reliability Standards as well as to evaluate and address the potential risk of a coordinated cyberattack on geographically distributed targets. As the Commission explained in the NOI, the "CIP Reliability Standards are intended to provide a risk-based, defense in depth (i.e., multiple, redundant "defensive" measures) approach to cybersecurity of the bulk electric system."[4] In an effort to address emerging issues and to improve the cybersecurity of the BES, the Commission has modified the CIP Reliability Standards several times since approving the first mandatory CIP Reliability Standards in 2008.[5] NRECA agrees that it is important for the CIP Reliability Standards to provide a baseline and framework against the evolving cyber threat landscape to ensure the security of the BES. However, NRECA is concerned that the Commission's consideration of

[4] NOI at P 2.

[5] *Id.*

additional changes to the CIP Reliability Standards while registered entities still are revising their compliance programs to address the most recent round of changes[6] creates a different set of risks.

NRECA respectfully asserts that it would be more effective for the Commission to (1) allow the industry to implement the changes required under revised Reliability Standards CIP-008-6, CIP-005-6, CIP-010-3, CIP-012-1, and CIP-013-1, and then (2) evaluate the effect of those changes on the overall security of the BES, before considering any additional revisions to the CIP Reliability Standards, especially as they apply to low impact BES Cyber Systems. NRECA and its members understand the importance of being prepared for the constantly evolving cyber threat landscape. However, instead of seeking comment on potential enhancements to the CIP Reliability Standards, NRECA suggests that the Commission consider seeking comment on viewing the current body of CIP Reliability Standards as a framework that allows utilities to make adjustments to their cybersecurity programs to address evolving cyber threats, without requiring continuously revised or new CIP Reliability Standards for every new issue or vulnerability.

A. The NIST Framework

According to the NOI, Commission staff identified three National Institute of Standards and Technology ("NIST") Framework Categories that may not be adequately addressed in the CIP Reliability Standards, and, thus, could reflect potential reliability gaps: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events.[7] NRECA provides the below responses to the Commission's questions

---

[6] *Disturbance Monitoring and Reporting Requirements Reliability Standard*, Order Granting Deferred Implementation of Certain NERC Reliability Standards, 171 FERC ¶ 61,052 (2020) (granting a three-month deferral of the implementation of Reliability Standards CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)), CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments), and CIP-013-1 (Cyber Security – Supply Chain Risk Management)).

[7] NOI at P 3.

concerning the three identified categories, their potential applicability to low impact BES Cyber Systems, and whether they are already addressed in the current Commission-approved Reliability Standards. As an initial matter, NRECA urges the Commission not to propose or direct revisions to the CIP Reliability Standards for low impact BES Cyber Systems. As explained in more detail below, applying the proposed enhancements to low impact BES Cyber Systems would exponentially increase costs and efforts without a corresponding increase in security to the BES. Further, it would be inconsistent with NERC's risk-based approach that the Commission has supported, which rightly recognizes that the same protections required for high and medium impact BES Cyber Systems are not warranted for low impact assets. This is especially true because, if high and medium impact BES Cyber Systems are properly protected under the CIP Reliability Standards, there is little to no gap in protection created by low impact BES Cyber Systems.

NRECA respectfully submits that the current Commission-approved Reliability Standards provide an excellent baseline and foundation for the cybersecurity of the BES. Within the current regulatory framework, responsible entities are audited regularly by the Electric Reliability Organization ("ERO") Enterprise and implement appropriate processes, procedures, and internal controls to assure compliance with their obligations under the CIP and other Reliability Standards. These processes, procedures, and internal controls are how entities address residual risks and assure the continued reliable, secure operation of the BES.

As the industry continues to mature its operations and security, the current regulatory framework should also mature such that it decreases focus on inefficient administrative obligations and increases focus on entities' implementing the most appropriate security controls for their operating environment. In particular, the current approach of CIP Reliability Standards constrains utilities unnecessarily while continued revisions create their own set of risks. NRECA appreciates

the Commission's analysis relative to the NIST Framework and respectfully suggests that the Commission consider how such a framework could be leveraged to mature and evolve the overall approach to the CIP Reliability Standards and enforcement thereof. For example, alternative approaches such as implementation of controls within the NIST Framework could be used to address residual risks. This would provide flexibility with respect to the existing constraints resulting from the current framework while creating margin to make risk-based improvements in other areas.

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.

1. 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?

The Commission-approved CIP Reliability Standards address NIST Framework Data Security Category ("PR.DS") 4 (requiring adequate capacity to ensure availability is maintained) and 6 (requiring integrity checking mechanisms to verify software, firmware, and information integrity). As an initial observation, NRECA notes that there are several types of confidential data that are important to the reliability and security of the BES. These include critical energy infrastructure information such as BES Cyber System Information ("BCSI") and operating reliability data that is considered confidential pursuant to the NERC Operating Reliability Data Confidentiality Agreement (*e.g.*, real-time operating and markets data). Across the body of Reliability Standards, several standards and requirements have been implemented to address the availability of these types of data as is necessary for grid security and reliability. These

requirements address PR.DS 4 by requiring entities to implement processes and controls to ensure data availability and include CIP-009-6, CIP-011-2, CIP-012-1, EOP-008-2, IRO-002-6, and TOP-001-4.

In particular, relative to BCSI, CIP-009-6 addresses PR.DS-4 for high and medium impact BES Cyber Assets through its requirements for back-up and restore processes for BES Cyber Systems, and explicitly includes through requirement R1.3 that these processes address the back up and storage of information required to recover functionality. This requirement ensures that the information required to restore high and medium impact BES Cyber Systems to a functioning operational state is protected and available in the event that it is needed to restore an applicable system to its typical function. Additionally, CIP-011-2 requirement R1.2 requires that information be protected while in storage, transit, and use, which creates defense-in-depth protections specifically for this type of data.

Further, relative to operating reliability data, EOP-008-2 requires that the responsible entities have both primary and back up Control Centers that do not depend upon each other to maintain compliance with applicable Reliability Standards. To meet the requirements of EOP-008-2, entities must have operating plans and associated controls that address and include information and data availability at both locations. These plans and controls are intended to ensure availability of the information necessary for grid security and reliability. Moreover, IRO-002-6 and TOP-001-4 also require entities to implement redundant and diversely routed data exchange capabilities, which also have the effect of ensuring availability.

Finally, in Order No. 866, the Commission ordered modifications to CIP-012-1 to "require protections regarding the *availability* of communication links and data communicated between

bulk electric system Control Centers."[8] These current and future Reliability Standards work together to ensure that essential data is available, visible, and recoverable to ensure grid operations, security, and reliability.

Relative to PR.DS-6, NRECA agrees with the Commission that CIP-010-3 requirement R1.6 addresses PR.DS-6 by requiring the verification of the identity of the software source and the integrity of the software obtained from the software source. It also addresses third party vendor performance and remote access monitoring. NRECA also notes that CIP-003-8 requirement R2 requires a myriad of controls for low impact BES Cyber Assets and that it is likely that the overall integrity of low impact BES Cyber Systems will benefit from these controls.

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

The CIP Reliability Standards when coupled with the additional Reliability Standards referenced above provide sufficient protections for low impact BES Cyber Systems as approved and should not be modified to address PR.DS-4 and PR.DS-6. The physical and electronic access controls required for low impact BES Cyber Systems provide sufficient information and integrity protection at the asset level. Further, the majority of obligations related to the availability of operating reliability data discussed above are imposed irrespective of the impact of the equipment. Rather, the requirement is that entities define what information they need to plan, operate, and recover systems and implement appropriate processes and controls to ensure that such data and information is available as necessary. Accordingly, additional requirements to address availability or integrity specifically as related to low impact BES Cyber Systems are unnecessary. Any further

[8] *Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers*, 170 FERC ¶ 61,031, at P 3 (2020) (emphasis in original).

requirements would be inconsistent with NERC's and the Commission's risk-based approach and require an enormous increase in personnel, management overhead, and training costs for low impact BES Cyber Systems without a commensurate increase in security.

3. *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.*

As discussed above, the Commission-approved CIP Reliability Standards adequately address the subcategories PR.DS-4 and PR.DS-6 for high, medium, and low impact BES Cyber Systems. The requirements for low impact BES Cyber Systems include perimeter-based controls that specifically mitigate against coordinated attacks against multiple sites. As a result, the risk associated with low impact BES Cyber Systems is sufficiently low to preclude the need to address these Data Security Subcategories.

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.

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

The Commission should not direct NERC to revise the CIP Reliability Standards to require that low impact BES Cyber Systems be covered Anomalies and Events Subcategories DE.AE-2 and DE.AE-4 because these subcategories are already addressed in CIP-003-6 requirements R1.2.4 and R2. Specifically, CIP-003-6 requirements R1.2.4 and R2 already require that registered entities have in place a Cyber Security Incident response policy and plan for assets identified in CIP-002-

5.1a containing low impact BES Cyber Systems. The requirements associated with the Cyber Security Incident response plan include those regarding identification, response, and reporting, activities which, by their very nature, require detection and an understanding of targets and methods and impact analyses.

To be able to respond to Cyber Security Incidents, organizations must have in place detection and evaluation methods to determine whether their networks or systems are malfunctioning or are experiencing an attempted or successful cyber intrusion. Entities are also required to have methods and processes to identify the scope and manner of the impact of the cyber intrusion. What is more, CIP-008-6 requirement R2 requires the reporting of these events to the Electricity Information Sharing and Analysis Center ("E-ISAC") and, if subject to the jurisdiction of the United States, to the United States National Cybersecurity and Communications Integration Center ("NCCIC"). Entities, therefore, must respond not only to the issue in its entirety, which requires an understanding of the impact, but they also must analyze and understand the event to be able to fully report it to the E-ISAC.

As a result of these requirements, entities are already performing obligations that would address Anomalies and Events Subcategories DE.AE-2 and DE.AE-4. Revising the CIP Reliability Standards to incorporate a more explicit requirement to address these Subcategories is purely an administrative errand and will not increase the security of the low impact BES Cyber Systems. Instead, it would serve only to divert resources that otherwise would be deployed to protect and secure other, more critical systems.

2. *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?*

As discussed above, the CIP Reliability Standards adequately address Anomalies and Events Subcategories DE.AE-2 and DE.AE-4 through CIP-003-6 requirements R1.2.4 and R2. While CIP-003-6 does not specifically address anomalous activity, to be able to identify an issue as a Cyber Security Incident, classify that issue as a Cyber Security Incident, and respond, entities must employ detection methods that serve to identify, evaluate, and capture anomalous activity. The foundation of any Cyber Security Incident response plan is monitoring for anomalies and other issues and having a process in place to evaluate any such observations once made. For this reason, the CIP Reliability Standards already address Anomalies and Events Subcategories DE.AE-2 and DE.AE-4 through CIP-003-6 requirements R1.2.4 and R2, which obligate entities to have a Cyber Security Incident response plan.

3. *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.*

See response to A2-3 above.

4. *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.*

While the CIP Reliability Standards do not specifically address anomalous activity, as stated above, the foundation of any Cyber Security Incident response plan is monitoring for anomalies and other issues and having a process in place to evaluate any such observations once made. Cyber Security Incident response plan requirements in both CIP-003-6 and CIP-008-6

require entities to develop and implement these types of plans for high, medium, and low impact BES Cyber Systems. While CIP-003-6 and CIP-008-6 do not specifically address anomalous activity, to be able to identify an issue as a Cyber Security Incident, classify that issue as a Cyber Security Incident, and respond, entities must employ detection methods that serve to identify, evaluate, and capture anomalous activity.

Further, NRECA notes that revisions to CIP-008-6 that will become effective on January 1, 2021 require the reporting of attempts to compromise high and medium impact BES Cyber Systems. These new requirements will ensure that the monitoring and reporting for high, medium, and low impact BES Cyber Systems is risk-based and that resource allocations are based on the potential impact that the cyber intrusion of an asset could have. For these reasons, NRECA respectfully submits that the current requirements appropriately address risk to the BES.

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.

1. 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?

As discussed above in the response to question A2, the Commission-approved CIP Reliability Standards adequately address Mitigation Subcategories RS.MI-1 and 2 for low, medium, and high impact BES Cyber Systems. Specifically, both CIP-003-8 and CIP-008-6 require that registered entities have processes to identify and handle/respond to compromised systems and attempts to compromise a system resulting in a cybersecurity event for low, medium,

or high impact BES Cyber Systems, as well as to report such issues to the E-ISAC and NCCIC. The requirements of CIP-003-8 and CIP-008-6 clearly require entities to identify, evaluate and either respond to or handle events as well as attempts to compromise.

While these Reliability Standards do not use the specific verbiage that is found in the NIST framework, inherent in handling and response is "containment" and "mitigation." Therefore, entities are already performing obligations that would address Mitigation Subcategories RS.MI-1 and RS.MI-2. Revising the CIP Reliability Standards to incorporate the specific verbiage used in these Subcategories is purely an administrative errand and will not increase the security of the BES.

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

The Commission-approved CIP Reliability Standards adequately address Mitigation Subcategory RS.MI-3 for low impact BES Cyber System through CIP-003-8 requirements R1.2.4 and R2. These requirements obligate registered entities to address Cyber Security Incident response for assets identified in CIP-002-5.1a containing low impact BES Cyber Systems from both a policy and process/plan perspective. The Cyber Security Incident response plans that are developed and implemented pursuant to CIP-003-6 requirement R2 must include procedures addressing incident identification, classification, response, and handling, to which incident containment, eradication, mitigation, and resolution are inherent.

While these CIP Reliability Standards do not use the specific verbiage that is found in the NIST framework, inherent in handling and response is "mitigation." Therefore, entities are already performing obligations that would address Mitigation Subcategory RS.MI-3. Revising the CIP

Reliability Standards to mimic the specific verbiage utilized in NIST framework is purely an administrative errand and will not increase the security of the BES.

B. Coordinated Cyberattack Assessment

NRECA understands the Commission's concerns regarding the potential for a coordinated cyberattack. However, it notes that substantial comments were submitted to NERC following its conclusions and recommendations in the December 9, 2019 Supply Chain Risk Assessment,[9] which comments were primarily focused on the basis for its conclusions and recommendations regarding the potential for a coordinated cyberattack. More specifically, NRECA would respectfully raise the following points for the Commission's consideration.

NRECA understands and supports the Commission's efforts to more fully examine the potential impact of a coordinated cyberattack. However, the current NERC position on such attacks is unsupported. In its Supply Chain Risk Assessment, NERC determined that a coordinated cyberattack with control of multiple low impact locations could result in an event that has an interconnection-wide BES reliability impact using only the number of asset locations without any analysis of actual location, proximity, magnitude (*e.g.*, MW, kV) or electrical configuration. In reality, the potential for such an impact is closely correlated with the actual geographic and electrical location of assets within an interconnection, their individualized, aggregate ability for impact within and beyond their local area, the overall electrical configuration within which such issue would arise, and other essential factors and characteristics. More finely put, ***neither number nor any of these factors alone*** are determinative of the likelihood or risk of an aggregate,

[9] NERC, Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf (Dec. 9, 2019).

interconnection-wide reliability impact. For this reason, NRECA provides the below responses to the Commission's questions concerning the risk of a coordinated cyberattack on the bulk electric system and the potential need for Commission action to address such risk.

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.

There are several processes, mechanisms, and organizations in place that can be used to evaluate, mitigate, protect against, and recover from potential geographically distributed coordinated cyberattacks. First, it is important to recognize that the CIP Reliability Standards include a comprehensive set of security controls that entities are required to apply to Cyber Systems based on risk. Relative to small, distributed resources, CIP-003-8 requirements R1.2.4 and R2 address the application of numerous security-focused processes and procedures that are intended to protect against geographically distributed cyberattack. This includes electronic and physical access controls, controls regarding use of removable media and transient Cyber Systems, and cybersecurity awareness. The ERO Enterprise audits add fidelity to these requirements on either a three- or six-year cycle, as do annual self-certifications.

Further, relative to evaluating, mitigating, and recovering from a geographically distributed cyberattack, both CIP-003-8 and CIP-008-6 require that registered entities identify Cyber Security Incidents and notify the E-ISAC of a Reportable Cyber Security Incident and/or a Cyber Security Incident that was an attempt to compromise an Applicable System. Further, if subject to the jurisdiction of the United States, these entities must also notify the NCCIC of any Reportable Cyber Security Incident and/or any Cyber Security Incident that was an attempt to compromise an

Applicable System. In addition to this CIP-008-6 reporting requirement, there is also a requirement for entities to complete and submit a Form OE-417 to the Department of Energy.

All of these reporting requirements result in important information sharing that enables other entities to become aware of issues and take proactive countermeasures. Further, use of the E-ISAC portal ensures that the E-ISAC can quickly communicate and provide insight into the mitigation of a widespread geographically distributed and coordinated cyber (and/or physical) attack. It is important to note that these reporting obligations allow agencies to perform internal threat assessments as well as to coordinate and collaborate with each other. This inter-agency collaboration is important as it facilitates trend identification and risk mitigation across the electric and other critical sectors.

Second, it is important to acknowledge the actions that the industry itself has undertaken to protect its assets from cyberattack. Over the last decade, utilities have gained both awareness and sophistication regarding cyber-related risks. While there is significant value in the government-industry partnership, utilities have also always found additional value through sector-specific partnerships and collaboration. Accordingly, there are several other threat-sharing organizations that disseminate information to the industry. These include Infragard, the Cyber Mutual Assistance Program, Regional Entity groups, third-party service providers, manufacturers/vendors and associated user groups, and the Cybersecurity Risk Information Sharing Program ("CRISP").

These organizations and collaborations create an effective community for intelligence sharing and, potentially, coordinating incident responses across the electric sector. Using these organizations and collaborations, smaller organizations can also benefit from the threat assessments that larger entities receive. Finally, such organizations and collaborations provide all

entities with the opportunity to share ideas, plans, and information such that the industry as a whole can more quickly leverage information-sharing to evolve and mature their operating processes and procedures collectively.

Third, the Reliability Standards require that registered entities plan, coordinate, and operate their systems with ongoing situational awareness. From the planning horizon to the real-time operations horizon, entities such as Regional Transmission Organizations, Reliability Coordinators, Balancing Authorities, and Transmission Operators are actively engaged in planning and operating the system using an N-1 contingency mindset and analysis. Studies, modeling, resource plans, and outage scheduling are all used to plan operations and to identify courses of action to take in response to different potential outage instances and combinations of outages.

Fourth, entities and market operators are required to ensure that they operate with the appropriate amount of reserves to withstand their most severe single contingency. These reserves and the planning that is necessary to operate and actively deploy reserves should be sufficient to comprise each entity's response to the loss of small, geographically distributed resources. Market operators employ other tools and products to provide support to the BES, such as fast-start and ramping products. As a further backstop, entities are also required to have system restoration plans and black start resources, which are coordinated and exercised annually. All of these operating plans and processes are more than sufficient to ensure the recovery of the BES from any outage, including those that may be caused by geographically distributed and coordinated cyberattacks.

Finally, in addition to these processes, mechanisms, and organizations, the Commission should acknowledge that resource investment is a significant investment for entities and, therefore, entities have considerable incentives to protect such investment through cybersecurity policies, procedures, and strategies. These include strategies such as "whitelisting," which only allows

specifically identified traffic through a firewall, "geo blocking," which restricts access to internet content based upon the user's geographical location, and other cybersecurity controls that prevent inbound and outbound connections to ensure that cyber risk is managed to an acceptable level.

When considered holistically, these processes, mechanisms, organizations, policies, procedures, and strategies provide ample evidence of operating processes and procedures that can be used to evaluate, mitigate, protect against, and recover from potential geographically distributed coordinated cyberattacks. Further, there is defense in depth, which greatly increases the likelihood that such processes and procedures will be both efficient and effective, whether in response to daily operating contingencies or recovery from a potential geographically distributed coordinated cyberattack.

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.

As discussed above, several of the processes, procedures, and mechanisms implemented to meet compliance with the CIP Reliability Standards result in the application of a comprehensive set of security controls to BES Cyber Systems that mitigate and protect against potential, geographically distributed, coordinated cyberattacks. CIP-003-8 requirements R1.2.4 and R2 require implementation of electronic and physical access controls, controls regarding use of removable media and transient Cyber Systems, and cybersecurity awareness. Further, both CIP-003-8 and CIP-008-6 require detection, identification, handling, and reporting of cyber intrusions and/or attempted intrusions. Implementation of these and other security measures by utilities (*e.g.*, geo-blocking, whitelisting) result in an effective "net" of security controls to evaluate, mitigate, and protect against potential geographically distributed coordinated

cyberattacks. This effectiveness and efficiency is further enhanced by the information sharing, threat intelligence sharing, and mutual assistance initiatives that the industry has embraced.

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?

Most of the processes, procedures and security controls described in response to questions B1 and B2 either are adequately addressed in the Commission-approved CIP Reliability Standards or relate to established collaborative processes. Organizations take security measures to supplement and complement these to ensure that their investments are adequately protected. NRECA respectfully submits that there are not any more processes, controls, or mechanisms that should or could be captured effectively through a new Reliability Standard or requirement without compromising the risk-based nature of the current set of Commission-approved Reliability Standards.

B4. What future changes to the bulk electric system design could affect the potential risks of geographically distributed coordinated cyberattacks?

As the Commission evaluates potential changes to the design of the BES, including policies governing the interconnection of distributed generation resources, the Commission should ensure it carefully considers reliability- and cybersecurity-related concerns as well as general policy concerns. The potential design and configuration of the BES and the interconnection of resources is one area of the Commission's jurisdiction that is addressed under both Section 205 and 215 of the Federal Power Act. This highly regulated area of the Commission's jurisdiction is required to be both reliable and just, reasonable and not unduly discriminatory or preferential. Therefore, transmission providers' policies must be carefully developed to ensure that they meet compliance

with the Reliability Standards without being unjust or unreasonable for interconnecting resources. Such is a delicate balance generally. However, in consideration of the Commission's question, such balance becomes even more delicate because distributed energy resources: (1) can be and often are interconnected at sub-transmission or distribution levels (*e.g.*, outside the scope of the Federal Power Act), which results in an intersection with state jurisdiction; (2) are eligible to interconnect through the small generator interconnection procedures under the Open Access Transmission Tariff; or (3) are interconnecting to a non-jurisdictional utility, etc. All of these considerations create complexity and challenges relative to identifying and requiring BES design changes that would be enforceable as well as just, reasonable, and not unduly discriminatory or preferential.

Even if BES design changes are feasible, the real-time operation of the BES has, is, and will continue to shift to accommodate the ongoing move towards distributed energy resources. The Commission has held technical conferences and gathered significant information regarding the management of this resource shift.[10] These inquiries clearly indicated a need to shift more than just BES design, with commenters focused on data availability from resource operators, visibility, dispatchability, and other issues. For these reasons, NRECA respectfully asserts that a more holistic approach is necessary to address the potential impacts of distributed energy resources generally. Once addressed from a cybersecurity risk perspective, the shift to smaller, distributed generation resources could enhance reliability by forcing a bad actor to attack more targets on a variety of different networks to create a significant event.

[10] *See, e.g.*, Distributed Energy Resources: Technical Considerations for the Bulk Power System, Commission Staff Report, Docket No. AD18-10-000 (issued Feb. 2018).; *Electric Storage Participation in Markets Operated by Regional Transmission Organizations and Independent System Operators*, Notice of Proposed Rulemaking, 157 FERC ¶ 61,121 (2016).

B5. Are current regional drill exercises and operator training effective in preparing to mitigate and recover from a geographically distributed coordinated cyberattack?

The current regional drill exercises and operator training are effective in preparing utilities to mitigate and recover from a geographically distributed coordinated cyberattack. These drills utilize various contingencies and emergency scenarios (natural and man-made) to allow entities to exercise their restoration plans and identify any obstacles, circumstances, or limitations within such plans and their associated assumptions. This provides the opportunity for entities and their personnel to exercise not only their training and plans, but also their coordination and cooperation with neighboring entities and their change management processes. Entities are able to define their exercise scenarios and – where there is significant distributed generation – an entity can exercise its plan specifically as it relates to recovery for an emergency arising out of the attack on or loss of such generation.

Further, entities do not just participate in their own or neighboring entity exercises, but they can also participate in additional exercises, such as regional and NERC Grid Security Exercises ("GridEx"). GridEx, which simulates cyberattacks and takes place every 24 months, have been helpful in considering the most effective responses to these types of cyberattacks. Further, regional power system restoration exercises regularly drill operators on how to recover from mass outage conditions and the current training established by NERC, the regional entities, and other organizations that focus on emergency operations, blackstart, and system restoration. All of these exercise options also provide the opportunities to develop lessons-learned and make related improvements to processes and plans.

1. *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?*

Current initial and refresher system operator training focuses on training system operators to recognize and respond to a wide range of scenarios and events regardless of whether their source is natural or man-made. This training includes cybersecurity awareness, how to recognize a cyber event, and how to respond to impacts on the grid when an event is occurring. Most importantly, however, system operator training focuses on ensuring that operators are trained and knowledgeable about how and when to respond to events happening on the grid, regardless of the event's source. At the outset of an event, an operator may simply see that a plant has gone offline or that its generation has changed. There may not be immediate visibility into the cause of a particular issue.

For this reason, system operators are trained on how to respond to keep the grid reliable and secure and to report anomalous events to operation and/or information technology personnel who are better equipped to evaluate and mitigate cyberattacks. It is important for system operators to be able to recognize and respond to a coordinated cyberattack. It is unrealistic to enforce mandatory training on this topic across the entire North American grid as the effectiveness of such training would be questionable. For these reasons, System Operators should continue to be trained to recognize and respond to a wide range of scenarios and events regardless of whether their source is natural or man-made, ensuring that such response is appropriately focused on awareness, notification, and confirmation of the event, and actions necessary for the stabilization of grid conditions.

> 2. *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?*

NRECA agrees with the Commission that it is important for all necessary personnel to receive the appropriate training and to exercise response and restoration plans. The current Commission-approved Reliability Standards require restoration and Cyber Security Incident response plans to be developed and maintained by responsible entities and to exercise those plans within a set periodicity. Initiation of these plans inherently include roles and responsibilities for system operations personnel and their leadership. Accordingly, associated training and exercises, which are typically scenario-based, also include participation by system operations personnel and their leadership. Further, participation in NERC's GridEx exercise continues to increase, and entities participate in regional power system restoration exercises once or twice per year.

> 4. *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?*

As discussed above, entities are required to train on and exercise their response and restoration programs within a set periodicity. Entities are able to define their exercise scenarios and – where there is significant distributed generation – an entity can exercise its plan specifically as it relates to recovery for an emergency arising out of the attack on or loss of such generation. It is unrealistic to enforce mandatory training on this topic across the entire North American grid as the effectiveness of such training would be questionable. Accordingly, NRECA does not believe that specific aspects of drill exercises or operating training pertaining to geographically distributed

coordinated cyberattacks need to be incorporated into the Reliability Standards. Entities should have the ability and discretion to mitigation of and recovery from a geographically distributed coordinated cyberattack in their training and exercises as is applicable to their operating area while also having the opportunity to focus on the risks more likely for their area.

Importantly, however, this scenario and the ability for an entity to exercise discretion within its area is one of the reasons why entity participation in exercises such as NERC's GridEx and other regional exercises continues to increase. Through these, entities can participate in the exercise of new, different, and broader scenarios across the interconnected nature of the BES. They have the opportunity to not only identify scenarios and impacts that had not been previously evaluated, but also to drill their personnel and their plans in response to such new, different, and broader scenarios and impacts. For these reasons, NRECA respectfully submits that utilities already have an incentive to participate in these types of drill exercises and operating training.

B6. Describe the effectiveness of industry information sharing at mitigating potential geographically distributed coordinated cyberattacks?

The available threat sharing platforms, including E-ISAC, CRISP, cyber mutual assistance, and other programs and organizations, are very effective at recognizing trends and sharing threat intelligence. E-ISAC effectively fulfills this role by actively sharing detailed, relevant alerts and bulletins to help industry mitigate potential geographically distributed cyberattacks. Information is shared on both cyber and physical security threats and risks for all member organizations across North America and includes indicators of compromise as well as effective mitigating actions. Similarly, but on a more localized basis, other regional, state, local and third-party service providers are effective in sharing information, which helps organizations mitigate potential geographically distributed coordinated cyberattacks.

The effectiveness of all information and threat intelligence sharing is dependent upon the availability and accuracy of information. This is an area where the Commission and other agencies are uniquely situated to assist entities with better assuring the security and reliability of the BES. In particular, the Commission, the Department of Homeland Security, the Department of Energy, and other agencies have and gain access to substantially greater volumes of information and have significantly more resources to evaluate, validate, and verify such information and threat intelligence. For these reasons, NRECA would respectfully request that the Commission work closely with other agencies to mature and evolve its information sharing relative to security and threat intelligence. Such enhancements and efforts would significantly increase the overall effectiveness of information sharing as well as the security and reliability of the BES.

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.

While the thresholds established in CIP-002-5.1a, Attachment 1, Section 2, do not specifically address the risk of a geographically distributed coordinated cyberattack, they are appropriate to ensure that registered entities address the highest risks to the BES, including the risk of a geographically distributed coordinated cyberattack. Further, CIP-002-5.1a R2.9 includes an allowance for a Reliability Coordinator, based on an engineering study of the region, to escalate the impact level of any facilities that could impose operating limits in an emergency condition. Given that a utility likely would need visibility beyond its own service territory to identify a geographically distributed cyberattack, a Reliability Coordinator is better positioned than an individual utility to identify and help address such operational challenges.

Looking forward, the existing set of CIP requirements is a good and necessary framework and baseline of security controls. However, rather than issuing a directive to NERC to add new

requirements to this framework, the Commission should look for opportunities to create flexibility within the body of CIP Reliability Standards where it would increase efficiency and promote security improvements as identified under a risk-based analysis.

IV. CONCLUSION

WHEREFORE, NRECA respectfully requests that the Commission consider its comments in evaluating potential enhancements to the Commission-approved CIP Reliability Standards.

Respectfully submitted,

NATIONAL RURAL ELECTRIC
COOPERATIVE ASSOCIATION

/s/ Barry R. Lawson
Barry R. Lawson
Senior Director, Regulatory Affairs

National Rural Electric Cooperative
Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5781

THOMPSON COBURN LLP

/s/ Jesse Halpern
Jesse Halpern

1909 K Street, N.W.
Suite 600
Washington, DC 20006
Telephone: (202) 585-6900

Counsel for National Rural Electric Cooperative Association

August 24, 2020