171 FERC ¶ 61,215
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. RM20-12-000]

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards

June 18, 2020

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Inquiry.

SUMMARY: The Federal Energy Regulatory Commission (Commission) seeks comment on certain potential enhancements to the currently-effective Critical Infrastructure Protection (CIP) Reliability Standards. In particular, the Commission seeks comment 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 comment 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.

DATES: Initial Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and Reply Comments are due **[INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.
- *Instructions*: For detailed instructions on submitting comments, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

Vincent Le (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6204
Vincent.Le@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
Kevin.Ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

171 FERC ¶ 61,215
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF INQUIRY

June 18, 2020

1. In this Notice of Inquiry (NOI), the Commission seeks comment on whether the currently-effective Critical Infrastructure Protection (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 comment 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.

2. The Commission-approved 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. Since the approval of the first mandatory CIP Reliability Standards in 2008, these standards have been modified on multiple occasions to address emerging issues and to improve the cybersecurity posture of the bulk electric

system.[1] Yet, new cyber threats continue to evolve, and the Reliability Standards should keep pace to maintain a robust, defense in depth approach to electric grid cybersecurity.

3. With this in mind, Commission staff undertook a review of the National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST Framework), which sets forth a comprehensive, repeatable structure to guide cybersecurity activities and to consider cybersecurity risks as part of an organization's risk management processes of its critical infrastructure.[2] Commission staff compared the content of the NIST Framework with the substance of the CIP Reliability Standards, and identified certain topics addressed in the NIST Framework that may not be adequately addressed in the CIP Reliability Standards. Commission staff further analyzed whether the identified topics are within the scope of the CIP Reliability Standards.[3] Commission staff then

[1] *See*, *e.g.*, *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016); *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032 (2018).

[2] NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 , Executive Summary at v, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[3] The NIST Framework provisions that pertain to business organization activity were not considered appropriate to address in the CIP Reliability Standards. For example, the NIST Framework provisions that pertain to the Governance Category (ID.GV) were not considered appropriate to be addressed in the CIP Reliability Standards since they address the policies, procedures, and processes to manage and monitor the

studied whether the potential "gaps" that are within the scope of the CIP Reliability Standards presented a significant risk to bulk electric system reliability. Based on this analysis, Commission staff identified the three NIST Framework categories that are the subject of this NOI: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events.

4. In addition, the Commission seeks comment on the risk of a coordinated cyberattack on the bulk electric system and potential Commission action to address such risk. In general, bulk electric system planning is based on the ability to withstand a system's single largest contingency, known as an N-1 event. The Commission has questioned whether greater defense in depth is warranted to better protect the bulk electric system from a coordinated attack on multiple BES Cyber Assets.[4] The risk of such a coordinated attack may be exacerbated by the recent shift from larger, centralized generation resources to smaller, more geographically distributed generation resources.

---

organization's regulatory, legal, risk, environmental, and operational requirements that inform the management of cybersecurity risk.

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at P 256, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No, 706-B, 126 FERC ¶ 61,229, *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009). NERC defines BES Cyber Asset as a "Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." Glossary of Terms Used in NERC Reliability Standards, http://www.nerc.com/files/glossary_of_terms.pdf.

The Commission seeks comment on the need to address the risk of a coordinated cyberattack on the bulk electric system, as well as potential approaches to address the matter, such as voluntary or mandatory participation in grid exercises, other types of training to prepare for a coordinated attack, and modifications to the current applicability thresholds in Reliability Standard CIP-002-5.1a that would subject additional facilities to the CIP controls that apply to medium and/or high impact BES Cyber Assets.[5]

I. Background

A. CIP Reliability Standards

5. In January 2008, the Commission issued Order No. 706, which approved the first set of mandatory CIP Reliability Standards addressing cybersecurity. In Order No. 706, the Commission stated *inter alia* that NERC should look to NIST as a source for improving the CIP Reliability Standards. The Commission also indicated that it may address the appropriateness of adopting NIST cybersecurity standards in the CIP Reliability Standards in a future proceeding:

[5] Reliability Standard CIP-002-5.1a (Bulk Electric System Cyber System Categorization) requires a registered entity to categorize its cyber systems in terms of low, medium, and high impact to the grid. These impact ratings determine which requirements in NERC Reliability Standards CIP-004 though CIP-013 apply to BES Cyber Systems. Attachment 1 of the Reliability Standards, "Impact Rating Criteria," identifies the criteria for identifying cyber systems as low, medium or high impact. For example, a control center used to perform the functions of a balancing authority for generation equal to or greater than an aggregate of 3,000 megawatts (MW) in a single interconnection is designated a high impact asset. A control center that performs the operations of a generator operator for an aggregate highest rated net real power equal to or exceeding 1,500 MW in a single interconnection is designated as a medium impact asset.

> The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. . . . Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, ...[6]

Moreover, although Order No. 706 did not directly address the issue of a potential coordinated attack on cyber assets, the Commission did express concern that focus on the N-1 planning principle may not be appropriate in the context of a cybersecurity because an attacker may simultaneously attack multiple assets. In particular, the Commission observed:

> While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk-based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset.[7]

---

[6] Order No. 706, 122 FERC ¶ 61,040 at P 233.

[7] *Id.* P 256.

6. NIST has continued to serve as an important source for the improvement of the CIP Reliability Standards. For example, in 2013, the Commission issued Order No. 791, which approved the CIP Version 5 Standards.[8] The CIP Version 5 Standards adapted a new approach to identifying BES Cyber Assets subject to the CIP Standards, categorizing such assets as of low, medium and high impact. NERC explained that it developed this tiered approach based on a review of NIST cyber security standards.[9]

B. The NIST Framework

7. The NIST Framework was developed in response to Executive Order 13,636 "Improving Critical Infrastructure Cybersecurity," issued on February 12, 2013.[10] The NIST Framework version 1.0 was released in February 2014 and revised version 1.1 was released in April 2018. Executive Order 13,636 stated that the NIST Framework was designed to "reduce cyber risks to critical infrastructure[,] . . . [and] shall include a set of standards, methodologies, procedures, and processes that align policy, business, and

[8] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[9] *See* Order No. 791, 145 FERC ¶ 61,160 at P 14. On August 26, 2019, the U.S. Government Accountability Office (GAO) submitted a report to Congress that addressed the completeness of the CIP Reliability Standards in comparison to the subject matter addressed in the NIST Framework as well as the risks to the electric grid from a coordinated cyberattack. GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid* (Aug. 2019), https://www.gao.gov/assets/710/701079.pdf.

[10] Exec. Order No. 13,636, 78 Fed. Reg. 11737 (Feb. 19, 2013).

technological approaches to address cyber risks[,] . . . [and] incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[11]

8. The NIST Framework consists of five Functions that each provide a high-level, strategic view of one part of an organization's cybersecurity risk management. The five Functions are:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;
- Protect – Develop and implement appropriate safeguards to ensure delivery of critical services;
- Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event;
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event; and
- Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

9. Each of the five Functions is composed of Categories and Subcategories, with the five Functions having a total of 23 Categories and 108 Subcategories. Categories are defined as cybersecurity outcomes closely tied to programmatic needs and activities. The 23 Categories that are organized within the five Functions, are as follows: (1) Identify Function (Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management); (2) Protect Function (Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Process and Procedures, Maintenance, and Protective

[11] *Id.* at 11741.

Technology); (3) Detect Function (Anomalies and Events, Security Continuous Monitoring, and Detection Process); (4) Respond Function (Response Planning, Communications, Analysis, Mitigation, and Improvements); and (5) Recover Function (Recovery Planning, Improvements, and Communications).

II. Discussion

A. The NIST Framework

1. Analysis

10. Based on a comparison of the NIST Framework and CIP Reliability Standards, Commission staff identified three 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.

a. Data Security Category

11. The NIST Framework Data Security Category (PR.DS) specifies activities to manage 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 Data Security Category identifies internal controls in eight Subcategories to require that: (1) data at rest is protected (PR.DS-1); (2) data in transit is protected (PR.DS-2); (3) assets are formally managed throughout removal, transfer, and disposition (PR.DS-3); (4) adequate capacity to ensure availability is maintained (PR.DS-4); (5) protections against data leaks are implemented (PR.DS-5); (6) integrity checking mechanisms are used to verify software, firmware, and information integrity (PR.DS-6); (7) the development and

testing environment(s) are separate from the production environment (PR.DS-7); and (8) integrity checking mechanisms are used to verify hardware integrity (PR.DS-8).[12]

12. Commission staff analysis indicates that two NIST Data Security Subcategories may not be adequately addressed in the CIP Reliability Standards. First, the Subcategory requiring adequate capacity to ensure availability is maintained (PR.DS-4) does not appear to be addressed in Reliability Standard CIP-011-2 (Information Protection) or Reliability Standard CIP-012-1 (Communications between Control Centers), which addresses real-time assessment and real-time monitoring data while being transmitted between any applicable control center. Reliability Standard CIP-011-2 addresses the confidentiality and integrity of medium and high impact BES Cyber System information, but it does not address availability of information and does not apply to low impact BES Cyber Systems. Reliability Standard CIP-012-1, which has not yet gone into effect, augments the data protection controls in the CIP Reliability Standard, but it is limited to real-time assessment and monitoring data transmitted between control centers.[13] The loss of BES Cyber System information availability could result in a loss of the ability to accurately maintain or restore the bulk electric system, which could affect reliability.

[12] *See* NIST Cybersecurity Framework at 32-33.

[13] In Order No. 866, the Commission approved Reliability Standard CIP-012-1 and also directed NERC to modify the Reliability Standard to require protections regarding the availability of links and data communicated between control centers. *Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications Between Control Centers*, Order No. 866, 170 FERC ¶ 61,031 (2020).

13. In addition, while integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6) are partially addressed by Reliability Standard CIP-013-1 (Supply Chain Risk Management), the requirements do not apply to low impact BES Cyber Systems, nor do they apply to information, such as a digital manual provided with a software tool, for low, medium, or high impact BES Cyber Systems. Not verifying software, firmware, and information integrity may allow a malicious actor to bypass existing security controls without detection.

14. In sum, the absence of CIP Reliability Standard requirements corresponding to Subcategories PR.DS-4 and PR-DS-6 in the NIST Framework could represent a potential gap in the CIP Reliability Standards.

b. Anomalies and Events Category

15. The NIST Framework Anomalies and Events Category (DE.AE) identifies security controls to detect anomalous activity and understand the potential impact of events. Specifically, the Anomalies and Events Category identifies internal controls in five Subcategories to require that: (1) a baseline of network operations and expected data flows for users and systems is established and managed (DE.AE-1); (2) detected events are analyzed to understand attack targets and methods (DE.AE-2); (3) event data are aggregated and correlated from multiple sources and sensors (DE.AE-3); (4) the impact of events is determined (DE.AE-4); and (5) incident alert thresholds are established (DE.AE-5).[14]

[14] *See* NIST Cybersecurity Framework at 37-38.

16. Reliability Standard CIP-008-5 (Incident Reporting and Response Planning) specifies incident response requirements to mitigate the risk to the reliable operation of the bulk electric system resulting from a cyber security incident.[15] This includes a requirement that applicable entities have a process to "identify, classify, and respond to Cyber Security Incidents," which corresponds to Subcategories DE.AE-2 and DE.AE-4.[16] However, Reliability Standard CIP-008-5 is only applicable to medium and high impact BES Cyber Systems. Accordingly, there is no requirement, similar to Subcategories DE.AE-2 and DE.AE-4, for low impact BES Cyber Systems. If a low impact BES Cyber System is compromised and an analysis is not performed, the compromised low impact BES Cyber System can potentially be used to gain access to other BES Cyber Systems, including medium and high impact BES Cyber Systems.

c. Mitigation Category

17. The NIST Framework Mitigation Category (RS.MI) specifies activities to prevent the expansion of a cybersecurity event, mitigate any effects and resolve the incident. The Mitigation Category identifies internal controls in three Subcategories to require that: (1) incidents are contained (RS.MI-1); (2) incidents are mitigated (RS.MI-2); and (3)

[15] Reliability Standard CIP-008-6, which becomes effective on January 1, 2021, expands the current version's scope to include Electronic Access Control or Monitoring Systems and suspicious activity, but it does not include low impact BES Cyber Systems.

[16] Reliability Standard CIP-008-5, Requirement R1.1.

newly identified vulnerabilities are mitigated or documented as accepted risks (RS.MI-3).[17]

18. Reliability Standard CIP-008-5 requires responsible entities to document their cybersecurity incident response plans and provide evidence of incident response processes or procedures that address incident handling. However, Reliability Standard CIP-008-5 does not specifically require incident containment or mitigation as discussed in Subcategories RS.MI-1 and RS.MI-2.[18] In addition, Reliability Standard CIP-008-5 does not apply to low impact BES Cyber Systems. Similarly, while Reliability Standard CIP-010-2 (Configuration Management and Vulnerability Assessments) addresses the need to mitigate newly identified vulnerabilities for medium and high impact BES Cyber Systems consistent with Subcategory RS.MI-3, it does not apply to low impact BES Cyber Systems. As noted above, without proper containment and mitigation, the compromise of a low impact BES Cyber System can potentially be used as a launching point to gain access to other BES Cyber Systems, including medium and high impact BES Cyber Systems.

2. Request for Comments

19. The Commission seeks comment on whether the currently effective CIP Reliability Standards adequately address aspects of the NIST Framework that support

[17] *See* NIST Cybersecurity Framework at 42-43.

[18] Reliability Standard CIP-008-6 also does not specifically address incident containment or mitigation.

bulk electric system reliability and associated operational technology (i.e., industrial control systems), as well as current and projected cybersecurity risks. As discussed above, there may be subcategories in the NIST Framework that are not adequately addressed in the CIP Reliability Standards, or addressed only with regard to medium and high impact BES Cyber Assets but not low impact BES Cyber Assets. While differences between the CIP Reliability Standards and the NIST Framework are to be expected, the Commission seeks comment on whether the differences identified herein reflect potential reliability gaps in the CIP Reliability Standards that should be addressed.

20. Below, we pose questions that commenters should address in their submissions. However, commenters need not address every topic or answer every question identified below.

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

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?

- 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?

- 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.

- 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.

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?

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

- 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.

B. Coordinated Cyberattack Assessment

1. Analysis

21. As discussed below, this NOI seeks comment on the risk of a coordinated cyberattack on the bulk electric system and the potential need for Commission action to address such risk.

22. Since the Commission approved the first mandatory CIP Reliability Standards in 2008, the generation resource mix has shifted away from larger, centralized generation resources to the expanding integration of smaller, geographically distributed generation resources. Accordingly, an increasing number of generation resources are categorized as low impact BES Cyber Systems, because they do not meet the thresholds in Reliability Standard CIP-002-5.1a for medium or high impact BES Cyber Systems, and therefore are not required to comply with the full suite of CIP Reliability Standards.[19]

23. In 2008, when the CIP Reliability Standards first became effective, it might have been more effective to focus cybersecurity protections on larger generation plants than smaller plants. However, given the shift to smaller generation resources, it is worth examining whether a sophisticated threat actor could initiate a coordinated cyberattack targeting geographically distributed generation resources, posing an unacceptable risk to

[19] Reliability Standard CIP-002-5.1a (Cyber Security – BES Cyber System Categorization), Attachment 1 (Impact Rating Criteria).

bulk electric system reliability. Such a coordinated cyberattack would present itself as a "common mode failure," which could be similar in risk to a wide-scale disruption to fuel supplies, such as an attack on a natural gas pipeline.

24. Recent publicly available studies and reports have assessed the potential reliability impacts of a coordinated cyberattack on geographically distributed targets. These sources evaluated the impact to the power grid from simultaneous or near simultaneous loss of geographically distributed electrical facilities that could result in widespread loss of electrical services, including long-duration, large-scale disturbances. The following three reports highlight the potential risks to Bulk-Power System reliability.

25. First, the NERC's 2019 Supply Chain Risk Assessment, based on information obtained through a mandatory data request to industry, concludes that a coordinated cyberattack "could greatly affect [bulk electric system] reliability beyond the local area."[20] The Supply Chain Risk Assessment examined the nature and complexity of cybersecurity supply chain risks, including those associated with low impact assets, and it found that:

> While [low impact] locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could affect BES reliability beyond the local area. The analysis of third-party electronic access to generation resource locations is even more concerning. More than 50% of all low impact locations of generation resources allow

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

> third-party electronic access. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly affect BES reliability beyond the local area.

Based on this assessment, NERC staff recommended that the Supply Chain Reliability Standards should be modified to include low impact BES Cyber Systems with remote electronic access connectivity.[21]

26. Second, on September 4, 2019, NERC published a Lessons Learned document regarding a denial-of-service attack against multiple remote generation sites whose BES Cyber Systems are categorized as low impact. The document explained that a known vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. The reboots resulted in a denial of service condition at a low impact control center and multiple remote low impact generation sites. This resulted in brief communications outages (i.e., less than five minutes) between field devices at the generation sites, as well as between the generation sites and the control center. Although the cyberattack did not cause a disturbance, it met the definition of a coordinated cyberattack, and it is possible that this

[21] *Id*. The NERC Board of Trustees adopted an alternative proposal to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems for malicious communications and vendor remote access, while continuing to evaluate the effectiveness and sufficiency of the supply chain risk management Reliability Standards. NERC, Resolution for Agenda Item 8.d: Supply Chain Recommendations (February 6, 2020), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Approved_Resolution_%20Supply%20Chain%20Follow%20Up%20(2-6-2020).pdf.

was the first coordinated cyberattack on the Bulk-Power System. The document recommended that "[e]ven in cases involving low-Impact BES assets, an entity should strive for good cyber security policies and procedures" by considering adopting security controls for low impact BES Cyber Assets above those required under the CIP Reliability Standards.[22]

27. Finally, on January 29, 2019, the United States Office of the Director of National Intelligence (ODNI) reported to the United States Senate Select Committee on Intelligence concerning potential nation state risks.[23] Specifically, the ODNI reported that:

> Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.[24]

28. In addition, ODNI reported that, "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[25] ODNI concluded

---

[22] NERC, Lesson Learned Risks Posed by Firewall Firmware Vulnerabilities, at 2-3 (Sept. 4, 2019).

[23] ODNI, Worldwide Threat Assessment of the US Intelligence Community (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[24] *Id.* at 5.

[25] *Id.* at 6.

that our nation state adversaries and strategic competitors will increasingly use cyber capabilities to, among other things, disrupt critical infrastructure.

29. The loss of power supply to an Interconnection can and has caused instability, uncontrolled separation, and cascading failures. Unreliable operations can be caused by either near simultaneous or sequential loss of facilities, which cause thermal, voltage, and/or stability limits to be violated. Simultaneous or near simultaneous loss of multiple facilities under 1,500 MW can cause these effects, which has been demonstrated historically[26] and through simulations.[27] The loss of even a single facility can cause thermal overloads on parallel facilities. Combined or sequential losses can trigger safety systems such as underfrequency load shedding relays to operate across the Interconnection which, in turn, could lead to instability and cascading outages. Based on the review of publicly available information discussed above, it is possible that such incidents could be caused by a coordinated cyberattack on geographically distributed targets.

2. Request for Comments

30. The Commission seeks comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether modifications to the CIP Reliability

[26] *See generally* U.S.-Canada Power System Outage Task Force, Final Report on the August 14 Blackout in the United States and Canada: Causes and Recommendations (April 2004), http://www.ferc.gov/cust-protect/moi/blackout.asp.

[27] *See*, *e.g.*, NERC, Frequency Response Initiative Report: The Reliability Impact of Frequency Response (October 30, 2012).

Standards, including potential modifications to the current MW thresholds, would be appropriate to address such risks. In particular, the Commission seeks comment regarding the procedures and security controls that are currently employed to protect against the potential risk of a geographically distributed coordinated cyberattack and whether modifications to the CIP Reliability Standards would be appropriate to address such risks.

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.

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.

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?

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

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

- 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?

- 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?

- 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?

- 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?

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

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?

III. Comment Procedures

31. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**], and Reply Comments are due [**INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. Comments must refer to Docket No. RM20-12-000, and must include the commenter's name, the organization they represent, if applicable, and their address.

32. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word-processing formats. Documents created electronically using word-processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

33. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

34. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

IV. Document Availability

35. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. eastern time) at 888 First Street NE, Room 2A, Washington, DC 20426.

36. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and

Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

37. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

Kimberly D. Bose,
Secretary.