Request for Information on the
Cyber Regulatory Harmonization

Office of the National Cyber Director Docket ID: ONCD-2023-0001

Comments of the North American Electric Reliability Corporation[1]

The North American Electric Reliability Corporation ("NERC") submits comments on the Office of the National Cyber Director's ("ONCD") Request for Information ("RFI") on opportunities for and obstacles to harmonizing cybersecurity regulations. NERC previously submitted joint comments with the six Regional Entities[2] to the Cybersecurity and Infrastructure Security Agency concerning harmonization of cyber incident reporting requirements. Accordingly, as requested, these comments exclude discussion of cyber incident reporting.

NERC appreciates the ONCD's efforts to harmonize cybersecurity regulations for critical infrastructure. As described below, pursuant to Section 215 of the Federal Power Act, the Federal Energy Regulatory Commission ("FERC") certified NERC as the Electric Reliability Organization ("ERO") charged with developing and enforcing mandatory reliability standards, including cybersecurity standards, applicable to owners, operators, and users of the Bulk Power System.[3] To that end, NERC respectfully requests that government agencies avoid duplication or conflict with NERC's set of mandatory and enforceable cybersecurity standards that apply to certain electric entities in the energy sector. The following comments describe NERC and its Regional Entities

[1] These comments are filed one day past the due date. NERC respectfully requests that the ONCD please accept these late-filed comments.

[2] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

[3] Under Section 215 of the Federal Power Act, FERC regulations, and the NERC Rules of Procedure, the Bulk Power System is defined as "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy." *See* 16 U.S.C. 824o(a)(1); 18 C.F.R. § 39.1; and NERC Rules of Procedure, Appendix 2, available at https://www.nerc.com/AboutNERC/RulesOfProcedure/ROP_Appendix%202_20220519.pdf.

and provide an overview of the CIP standards and their relationship to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, exemplifying harmonization of existing NERC Reliability Standards and the framework.

I. Description of NERC and the ERO Enterprise

NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the North American Bulk Power System. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

In the United States, FERC certified NERC as the designated ERO under Section 215 of the Federal Power Act. As the ERO, NERC is charged with developing and enforcing mandatory Reliability Standards applicable to owners, operators and users of the Bulk Power System; assessing current and future reliability trends; analyzing system events; and recommending improved practices. NERC accomplishes its mission with the support of the six Regional Entities. The six Regional Entities support reliability across differing interconnections with specific needs and characteristics by conducting compliance monitoring, enforcement, analysis, and outreach activities, among other things. Collectively, NERC and the six Regional Entities comprise the "ERO Enterprise."

NERC's mandatory and enforceable Reliability Standards, which are approved by FERC in the U.S., define the reliability requirements for planning and operating the North American Bulk Power System. NERC's Reliability Standards include a family of standards, referred to as the Critical Infrastructure Protection ("CIP") standards, which address cyber and physical security risks. The CIP standards provide a foundation of sound security requirements across the North American Bulk Power System. The CIP Reliability standards are unique in being some of the first

mandatory and enforceable cybersecurity policy and control requirements applied to non-governmental entities to protect critical infrastructure. Subject to FERC approval, NERC has the authority to sanction entities for violations of its mandatory standards. The CIP Reliability Standards include requirements applicable to the following types of electricity sector participants included on NERC's Compliance Registry: Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners.[4]

In addition to its role of developing and enforcing mandatory Reliability Standards, NERC also operates the Electricity Information Sharing and Analysis Center ("E-ISAC") on behalf of the electricity industry. The E-ISAC provides its members and partners with resources to enhance situational awareness, disseminates threat intelligence, and enables the reduction of cyber and physical security risks to the North American electricity industry.

II. Comments

a. Overview of CIP Standards

Drawing on concepts from the NIST Cybersecurity Framework, NERC's CIP cyber security standards provide risk-based security requirements across the North American Bulk Power System. The level of controls required for protecting cyber systems is in proportion to the risk each system presents to reliable operation of the Bulk Power System. This risk-based construct requires applicable entities to identify and categorize cyber systems based on the adverse impact that loss, compromise, or misuse of those systems could have on Bulk Power System reliability. Once these cyber systems are identified and categorized, the CIP standards require applicable entities to establish plans, protocols, and controls to protect these systems, address supply chain

[4] These terms are defined in NERC's Glossary of Terms Used in NERC's Reliability Standards, available here: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

risk management, train personnel on security matters, report security incidents, and recover from events, among other requirements. In addition, one CIP standard covers physical security of critical facilities.[5] The complete list of CIP standards is identified below.[6]

- Cyber System Identification and Categorization (CIP-002)
- Security Management Controls (CIP-003)
    - Including requirements for lower risk cyber systems (CIP-003)
- Personnel and Training (CIP-004)
- Electronic Security Perimeters (CIP-005)
- Physical Security of Cyber Systems (CIP-006)
- Systems Security Management (CIP-007)
- Incident Reporting and Response Planning (CIP-008)
- Recovery Plans (CIP-009)
- Change Management and Vulnerability Assessments (CIP-010)
- Information Protection (CIP-011)
- Communication Between Control Centers (CIP-012)
- Supply Chain Risk Management (CIP-013)
- Physical Security (CIP-014)

b. Avoid Duplication or Conflict with CIP Standards

As discussed above, certain electricity sector entities must comply with NERC's CIP standards, which provide a common foundation of essential security practices supporting reliability of the Bulk Power System. Violations of NERC standards are subject to a maximum penalty of $1,496, 035[7] per violation, per day. It is crucial that government agencies recognize the effective regulatory framework that is currently in place for the electricity sector to develop and

[5] These facilities include transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. *See* CIP-014-3, available at CIP-014-3.pdf (nerc.com).
[6] The NERC Reliability Standards are available at https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.
[7] The maximum penalty is an inflation-adjusted number subject to change.

enforce cyber security standards, and the complex, robust suite of mandatory, enforceable cyber security standards that are currently in place.

To avoid undue burden on the energy sector and given the potential negative consequences of regulatory complexity for entities, government agencies should avoid duplication or conflict with the existing and maturing CIP Reliability Standards. For instance, duplicating requirements without incorporating efficiencies in demonstrating compliance could divert resources from maintaining security to simply managing the increased compliance workload. In addition, development of any new cyber regulations needs to consider the unique structure and interconnectedness of the Bulk Power System in working to ensure that those regulations do not inadvertently conflict with existing CIP Reliability Standards, particularly when CIP Reliability Standards may provide a higher level of security than baseline standards applicable to all categories of critical infrastructure.

c. Third-Party Frameworks – NIST Cybersecurity Framework

NERC emphasizes its continued reliance on the NIST Framework to inform its cyber security activities, including future standards development and efforts to support effective implementation of enforceable Reliability Standards. The NIST Framework and the CIP Reliability Standards serve different purposes, however. Whereas the NIST Framework is voluntary guidance for non-governmental entities, the NERC CIP Reliability Standards are mandatory and enforceable for applicable entities in the electric sector. Accordingly, NERC uses concepts from the NIST Framework that are suited to developing auditable CIP requirements. For example, the currently enforceable CIP standards adopted the concept of categorizing cyber systems based on risk, then applying controls commensurate with that risk, from the NIST

Framework. As such, there will not be a complete overlap from the voluntary framework to the CIP requirements.

Nonetheless, NERC recognizes the importance of the NIST Framework and works to ensure the NIST Framework's voluntary guidance is taken into consideration and harmonizes with all CIP Reliability Standards. To that end, ERO Enterprise staff and NIST staff, with contributions from a working group of NERC's Reliability and Security Technical Committee ("RSTC"), developed an updated mapping of enforceable CIP Reliability Standards to the NIST Framework.[8] Through this exercise, NERC and NIST staff demonstrated a consistent mapping between CIP Reliability Standards and the NIST Framework, demonstrating harmonization.

III. Conclusion

NERC appreciates the opportunity to comment on the RFI and looks forward to continued coordination.

Respectfully submitted,

/s/ Marisa Hecht
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: November 1, 2023

[8] The mapping document has been added to the NIST Computer Security Resource Center National Online Informative References Program, available at National Online Informative References Program | CSRC (nist.gov) https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=90#/. The full mapping is available at: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/NIST%20CSF%20to%20NERC%20CIP%20OLIR%20Mapping.xlsx.