UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RR19-7-___**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO ORDER ON COMPLIANCE FILINGS FOR THE FIVE-YEAR PERFORMANCE ASSESSMENT

The North American Electric Reliability Corporation ("NERC") hereby submits this compliance filing in accordance with the Federal Energy Regulatory Commission's ("FERC" or "Commission") January 19, 2021 Order on Compliance Filings ("Order on Compliance Filings").[1] In that order, the Commission (1) accepted NERC's compliance filings, including modifications to the NERC Rules of Procedure ("ROP"), submitted in accordance with the Commission's order accepting NERC's 2019 Five-Year Performance Assessment,[2] and (2) directed NERC to submit an additional compliance filing to: (i) further clarify information sharing between NERC and the E-ISAC as it relates to the development of Reliability Standards; and (ii) revise its ROP to explicitly require that NERC share all Electricity Information Sharing and Analysis Center ("E-ISAC") All Points Bulletins ("APBs") with the Commission no later than at the time of issuance.[3]

This compliance filing is organized as follows: Section I of this compliance filing provides additional clarification regarding information sharing between NERC and the E-ISAC as it relates to the development of Reliability Standards; and Section II discusses the proposed revisions to Section 1003 of the ROP to require NERC to provide all E-ISAC APBs to the Commission. NERC

---

1 *N. Am. Elec. Reliability Corp.*, 174 FERC ¶ 61,030 (2021) [hereinafter *Order on Compliance Filings*].
2 *N. Am. Elec. Reliability Corp.*, 170 FERC ¶ 61,029 (2020) [hereinafter *Performance Assessment Order*].
3 *Order on Compliance Filings* at P 1-2.

requests that the Commission accept this compliance filing and approve the proposed revision to Section 1003 of the NERC ROP effective upon Commission approval.

I. Information Sharing Between the E-ISAC and NERC Regarding Reliability Standards Development

a. Background

As part of its 2019 Performance Assessment Report, NERC described its operation of the E-ISAC and its continued efforts to enhance the E-ISAC's value to industry participants.[4] The E-ISAC, created in 1999 pursuant to a U.S. presidential directive, provides its member utilities and partners with resources to prepare for and reduce cyber and physical security threats to the North American electricity industry. As NERC noted in its Performance Assessment Report, it has long recognized the importance of promoting robust information sharing between the E-ISAC and electricity industry participants to enhance industry's situational awareness and ability to prepare for and respond to cyber and physical security threats, vulnerabilities, and incidents.[5]

NERC also explained that to promote such a robust information sharing environment, it needed to institute a policy to separate the E-ISAC functions from other NERC program areas.[6] In short, because of NERC's responsibilities for the development and enforcement of mandatory Reliability Standards, there were concerns that electric industry participants would be hesitant to share information with the E-ISAC voluntarily out of fear that the information would be referred to NERC's Compliance Monitoring and Enforcement Program ("CMEP").[7] To address such concerns and to promote a robust information sharing environment, NERC explained that it

---

4 *N. Am. Elec. Reliability Corp.*, Docket No. RR19-7-000, July 22, 2019 at 13-17 [hereinafter Performance Assessment Report].

5 *Id*. at 14.

6 *Id*.

7 *Id*.

adopted a strict Code of Conduct in 2014 to govern the E-ISAC's relationship with other NERC departments and outline the parameters within which E-ISAC personnel may share information outside of the E-ISAC.[8]

NERC explained that the Code of Conduct sets out broad information sharing restrictions such that much of the information the E-ISAC receives from its member utilities voluntarily cannot be used across the Electric Reliability Organization ("ERO") to inform the development of Reliability Standards or the CMEP.[9] In accordance with the Code of Conduct and subject to limited exceptions, the E-ISAC cannot share member-provided information with other NERC departments unless that information has been anonymized and aggregated with other information (or the member utility consents to attributable sharing).

In its Performance Assessment Order, FERC sought "a better understanding of how the E-ISAC informs the development of Reliability Standards."[10] FERC directed NERC to provide "additional information on: (1) how NERC receives information from the E-ISAC and how the E-ISAC determines what data to share with NERC; and (2) once NERC receives such information, what NERC does with the information and how NERC determines whether such information is used to develop or inform the development of Reliability Standards."

On June 1, 2020, NERC submitted a compliance filing providing additional detail on the E-ISAC Code of Conduct and information sharing between the E-ISAC and NERC personnel involved in Reliability Standards development.[11] NERC reiterated that while the primary focus of the Code of Conduct is to ensure that information shared with the E-ISAC is not shared with,

---

8 *Id*. at 14-16.

9 *Id*.

10 *Performance Assessment Order* at P 68.

11 *N. Am. Elec. Reliability Corp.*, Docket No. RR19-7-001, June 1, 2020 at 20-24 [hereinafter First Compliance Filing].

reported to, or used by CMEP personnel to enforce NERC Reliability Standards, the Code of Conduct information sharing restrictions go beyond a simple restriction on conveying violation information to CMEP personnel. To promote robust information sharing within the electric industry, the E-ISAC Code of Conduct establishes broad information sharing restrictions, generally restricting E-ISAC personnel from sharing any information provided by a member utility voluntarily with any non-E-ISAC personnel at NERC, including NERC Reliability Standards development personnel, without the consent of the member utility.[12]

NERC clarified, however, that consistent with the Code of Conduct, the E-ISAC may share with other NERC program areas any of its reports, postings, or other issuances that anonymize and aggregate information provided by member utilities or other partners.[13] Such issuances would include, for example, threat trending analyses or analyses of specific threats, vulnerabilities, or risks so long as those reports do not include any attributable member-provided information or are based on information obtained from sources other than a member utility (e.g., government reporting or open source reports). NERC also noted that the Code of Conduct allows the E-ISAC to share mandatory reports submitted to the E-ISAC, such as reports required under the CIP-008 Reliability Standard, with Reliability Standard development personnel.

In its June 2020 compliance filing, NERC also described its efforts to enhance the E-ISAC's coordination with Reliability Standards development personnel.[14] NERC stated that it would establish a regular feedback loop between the E-ISAC and Reliability Standards development personnel through quarterly meetings. At these meetings, NERC stated that the E-ISAC and Reliability Standards personnel will share information and observations on security

12 *Id*. at 21-22.
13 *Id*. at 22-23.
14 *Id*. at 23-24.

threats, vulnerabilities, incidents and trends to help inform standards development activities, to the extent permitted by the E-ISAC Code of Conduct.[15]

NERC also stated that ERO Enterprise[16] subject matter experts for the Critical Infrastructure Protection ("CIP") Reliability Standards would review the information from the E-ISAC to perform a reliability gap analysis. The analysis would evaluate the E-ISAC-provided information to determine whether any modifications to the CIP standards are necessary to address a security risk.[17] NERC noted that if staff identifies a potential gap in the CIP Reliability Standards, NERC would either informally review the matter with industry to gather more information or initiate a Standard Authorization Request to formally begin a Reliability Standards development project.[18]

In its Order on Compliance Filings, the Commission directed NERC to "further clarif[y] information sharing between NERC and the E-ISAC, including the gap analysis process" referenced in NERC's June 2020 compliance filing.[19] The following section provides additional discussion regarding the exchange of information between the E-ISAC and NERC's Reliability Standards development personnel.

b. E-ISAC–NERC Reliability Standards Department Information Exchange

Consistent with its commitments in its June 2020 compliance filing, NERC established a regular information exchange between the E-ISAC and NERC CIP standards development personnel. As discussed below, the information exchange consists of (1) monthly meetings

15 *Id*. at 23.
16 The ERO Enterprise refers to NERC and the Regional Entities.
17 *First Compliance Filing* at 23-24.
18 *Id*.
19 *Order on Compliance Filings* at P 2.

between E-ISAC personnel and NERC CIP standards development personnel, and (2) the sharing of relevant E-ISAC issuances with NERC CIP standards development personnel.

Monthly Meetings: E-ISAC physical and cyber security analysts have begun to meet with Reliability Standards staff and CIP subject matter experts on a monthly basis to discuss the security threat landscape.[20] They share information and insights on recent threats and vulnerabilities; general security trends; adversary tactics, techniques, and procedures (or "TTPs"); and mitigation measures and tools. The agenda for each of these monthly meetings includes discussion of physical and cyber security threats/incidents from the previous month, overall security trends, and other items of interest. In each case, E-ISAC personnel take care to only share information consistent with the Code of Conduct (i.e., member-provided information that is anonymized and aggregated or information otherwise not subject to the Code of Conduct restriction, such as a CIP-008 report).

E-ISAC Issuances: In addition to these monthly discussions, the E-ISAC has begun to regularly share its reports, portal posts, APBs, and other issuances with NERC'S CIP standards development personnel when the Code of Conduct permits such sharing. As noted in the June 2020 compliance filing, the Code of Conduct permits the E-ISAC to share reports or other issuances that include member-provided information if that information is anonymized and aggregated (e.g., trending analyses) or issuances that do not include member-provided information (e.g., a report on or an analysis of a specific threat or vulnerability provided by government partner or security vendor).

The following section addresses NERC's use of E-ISAC-provided information to inform Reliability Standards development.

[20] In its June 2020 compliance filing, NERC stated the meetings would occur at least on a quarterly basis. NERC has decided to hold these meetings on a monthly basis to increase the frequency of interaction.

c. Evaluation of E-ISAC-Provided Information to Inform Reliability Standard Development

As discussed below, NERC personnel involved in CIP standards development use the information discussed during the monthly meetings and derived from E-ISAC issuances, along with information from other sources,[21] to inform CIP standards development. NERC uses E-ISAC-provided information to enhance active standard development projects and more broadly evaluate the adequacy of the CIP standards to address new and emerging security risks (i.e., to perform a gap analysis).

As it relates to active standards projects, NERC Reliability Standards development personnel use information available to them, from the E-ISAC or other sources, to advise active Standards Drafting Teams ("SDTs"). NERC's Reliability Standards development personnel have begun to share their observations and insights from the E-ISAC-provided information with active SDTs. The objective is to improve the CIP standards development process by using the E-ISAC-provided information, along with information from other sources, to provide SDTs greater awareness of the evolving threat landscape, recent security threats and vulnerabilities, adversary TTPs, and effective mitigation measures and best practices. The E-ISAC-provided information also serves as another data point that NERC's CIP subject matter experts use to evaluate an SDT's proposed modifications to the CIP standards.

Additionally, as noted above, NERC'S Reliability Standards development personnel use the E-ISAC-provided information to broadly evaluate the adequacy of the CIP standards in addressing emerging security threats and vulnerabilities. The initial step in this gap analysis process involves NERC's CIP subject matter experts discussing the E-ISAC-provided information,

[21] Other information sources include, among other things, lessons learned from compliance monitoring activities, open source material, and government or private sector reporting on security risks and best practices.

together with security information from other sources, to identify whether the information indicates there are any emerging security risks not currently addressed in the CIP standards adequately or otherwise indicates a gap in the CIP standards. NERC's CIP subject matter experts assess whether the CIP standards would, by design or implementation, help mitigate the risk and to what extent.

If the CIP subject matter experts identify a potential gap in the CIP standards in their initial review of the information, NERC would take steps to further explore the need for modifications to the CIP standards. Depending on the need for more information or better understanding of the matter, NERC has several options for further exploring the issue. It could, among other things, initiate an informal review of the information with industry, Regional Entity, and Commission subject matter experts; request that a NERC stakeholder committee (e.g., the Reliability and Security Technical Committee) evaluate the issue and produce a formal recommendation; or submit a Standard Authorization Request ("SAR") to the NERC Standards Committee to initiate a formal standards development project.

This gap analysis process is not new or unique to E-ISAC-provided information. NERC continually evaluates the adequacy of its CIP standards based on lessons learned from compliance monitoring activities, government reporting, security vendor reporting, and other information sources. The E-ISAC-provided information is another data point for SDTs and the ERO Enterprise CIP subject matter experts to evaluate the efficacy of the CIP standards in reducing physical and cyber security risks to the Bulk-Power System ("BPS").

The information exchange between the E-ISAC and NERC CIP standards development personnel related to the recent supply chain compromise involving SolarWinds provides an example of this process in action. Following the disclosure of the supply chain compromise in

December 2020, the E-ISAC began to gather and analyze information about the incident from various sources – including security vendors, government partners, member utilities, and cross-sector partners – and share relevant information about the incident to help support industry's response. The E-ISAC shared the information via its secure portal and through webinars/conference calls.[22]

Concurrently, NERC's CIP standards development personnel were also learning about the compromise. While the E-ISAC was focused on increasing situational awareness to help support industry's immediate response to the incident, NERC CIP standard development personnel were focused on understanding the incident to evaluate the adequacy of the CIP standards to mitigate the impact of such an attack on BPS reliability and apply lessons learned to CIP standards development activities involving supply chain risk management.

At their first monthly meeting following disclosure of the incident, the E-ISAC and NERC CIP standards development personnel discussed the incident, sharing insights and observations regarding the information known at that time. At subsequent monthly meetings, E-ISAC and Reliability Standards development personnel continued to share information about the incident as new or updated information about the incident and mitigation measures became available. During this time, the E-ISAC also shared many of its portal posts and other documents related to the incident with NERC CIP standards development personnel.

All of this information sharing was accomplished within the parameters of the E-ISAC Code of Conduct. While the Code of Conduct prohibited the E-ISAC from sharing information supplied by a member utility voluntarily, including information regarding a member's exposure to the vulnerability and impact on its environments, the E-ISAC and CIP subject matter experts

[22] The E-ISAC continues to track this incident and share updated information with its member utilities and partners.

exchanged information relevant to CIP standards development, including, among other things, the nature of the incident; the TTPs used by the attackers; whether the attackers could use the supply chain compromise to gain access to and operational control over environments subjects to the CIP standards; and recommended mitigation measures for organizations exposed to the vulnerability. The E-ISAC was also able to share high level, aggregated information about the extent of conditions in the electricity sector. The E-ISAC and NERC Reliability Standards personnel continue to exchange information on the incident as new information becomes available that would be relevant to CIP standards development and may be shared under the Code of Conduct.

Using the E-ISAC-provided information, among other data points, NERC's CIP subject matter experts are in the process of evaluating whether the CIP standards require modifications to further reduce the risk that such a supply chain compromise could adversely affect environments subject to the CIP standards. At this time, no decision has been made to submit a SAR or initiate another formal process to evaluate CIP standard modifications. NERC, however, has initiated informal discussions among ERO Enterprise subject matter experts and stakeholders regarding the need for CIP standard modifications to address evolving supply chain threats.

This evaluation and stakeholder discussions are occurring within the context of existing efforts to study the efficacy of the existing supply chain risk management requirements in the CIP standards. In August 2017, when the NERC Board of Trustees ("Board") adopted the supply chain risk management requirements in Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1, the Board concurrently adopted additional resolutions related to their implementation and evaluation.[23] The resolutions outlined six actions, developed by NERC management and

[23] The resolutions are available here: https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

stakeholders, to assist in the implementation and evaluation of the Supply Chain Standards and other activities to address potential supply chain risks for assets not currently subject to the Supply Chain Standards.[24]

Additionally, at its February 2021 meeting, the Board approved the withdrawal of proposed Reliability Standard CIP-002-6 that was pending before the Commission in recognition that "recent cybersecurity events and the evolving threat landscape warrant additional caution regarding any criteria that may permit more entities to categorize BES Cyber System as low impact and therefore subject to fewer requirements in the CIP Reliability Standards."[25] The Board directed NERC management to review the risk categorization criteria in CIP-002 in light of the recent supply chain compromises, among other things, to determine whether such criteria should be modified. E-ISAC-provided information will help inform both the study on the efficacy of the existing supply chain risk management requirements and the review of the CIP-002 criteria.

As NERC learns more about the recent supply chain compromises, studies the efficacy of the existing supply chain risk management requirements, and evaluates the criteria in CIP-002 in accordance with NERC's Board of Trustees resolution, NERC may initiate a formal process to assess proposed revisions to the CIP standards to further address supply chain risks. As this

[24] Pursuant to the Board's resolutions, NERC initiated the Supply Chain Risk Mitigation Program. As part of this program, NERC plans to measure the effectiveness of the supply chain standards during their first two years of implementation. At a high level, NERC plans to: (1) conduct surveys on supply chain awareness to inform analysis of trends; (2) compare contract language provided voluntarily by entities; (3) review audit and compliance information to determine whether language is clear or whether there are any reliability gaps; and (4) evaluate successful communication of supply chain vulnerabilities. NERC staff plans to report to the NERC Board of Trustees periodically on these activities during the first two years of implementation, as necessary. Additional information on the Supply Chain Risk Mitigation Program is available at: https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

[25] The Board's February 2021 resolutions are available here: https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/00-Board-Open-Meeting_Draft_Minutes-Feb-4-2021.pdf.

evaluation occurs, NERC's CIP subject matter experts are already using the E-ISAC-provided information to advise active SDTs.

II. Revisions to Section 1003 of the NERC ROP

a. Background

In the Performance Assessment Order, the Commission directed NERC "to clarify its processes regarding the development and issuance of [APBs]."[26] Consistent with that directive, in its September 28, 2020 compliance filing, NERC explained the process for the development and issuance of APBs and the factors the E-ISAC considers in deciding whether to issue an APB and whether to do so in conjunction with a NERC Alert or another form of communication. In its Order on Compliance Filings, the Commission found that NERC's explanation addressed the Commission directive to clarify its APB processes.[27] Nevertheless, the Commission directed NERC to "modify its [ROP] to explicitly require NERC to share all APBs with the Commission no later than the time of issuance."[28]

b. Proposed ROP Revisions

Consistent with the Commission's directive, NERC proposes to revise Section 1003 of the ROP to include a provision requiring NERC to share all APBs with Commission staff no later than at the time of issuance. Section 1003 of the ROP describes NERC's infrastructure security program, including, among other things, its operation of the E-ISAC. NERC proposes to add the following provision in Section 1003:

> As part of the E-ISAC's efforts to fulfill its mission, it may issue, as circumstances warrant, written communications, referred to as All Points Bulletins (APBs), to disseminate critical security information rapidly to electricity sector asset owners and operators as security threats and attacks develop, and critical, time-sensitive security information becomes available. *The E-ISAC shall share all APBs with*

---

26 *Performance Assessment Order* at P 68 n.89.
27 *Order on Compliance Filing* at P 38.
28 *Id.*

Federal Energy Regulatory Commission staff no later than at the time of issuance. (Emphasis added)

The proposed change reflects NERC's current practice of sharing APBs with Commission staff at the time of issuance. When possible, the E-ISAC provides Commission staff drafts of the APBs in advance of issuance and will continue that practice as circumstances permit.

Clean and Redline versions of the proposed revisions to ROP Section 1003 are included as Attachments A and B hereto, respectively.

III. Conclusion

For the reasons set forth above, NERC requests that the Commission accept this compliance filing and approve the proposed revisions to Section 1003 of the NERC ROP, effective upon Commission approval.

Respectfully submitted,

/s/ Shamai Elstein
Shamai Elstein
Associate General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
shamai.elstein@nerc.net

Counsel for North American Electric Reliability Corporation

Date: May 19, 2021

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding. Dated at Washington, D.C. this 19th day of May 2021.

/s/ Shamai Elstein

Shamai Elstein

Counsel for North American Electric Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment A

Proposed Revisions to ROP Section 1003
Clean

1003. Infrastructure Security Program

NERC shall participate in and, where appropriate, coordinate electric industry activities to promote Critical Infrastructure protection of the Bulk Power System in North America. NERC shall, where appropriate, take a leadership role in Critical Infrastructure protection of the electricity sector to help reduce vulnerability and improve mitigation and protection of the electricity sector's Critical Infrastructure. To accomplish these goals, NERC shall perform the following functions.

1. Electricity Information Sharing and Analysis Center (E-ISAC)

    1.1 NERC shall operate the E-ISAC on behalf of the electricity sector. In 1998, the U.S. Secretary of Energy asked NERC to serve as the information sharing and analysis center for the electricity sector, in implementation of Presidential Decision Directive 63, as part of a public/private partnership to deal with matters related to infrastructure security.

    1.2 The E-ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity sector, across interdependent sectors, and with government partners. The E-ISAC, in collaboration with the United States Department of Energy (DOE) and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

    1.3 NERC shall improve the capability of the E-ISAC to fulfill its mission.

    1.4 NERC shall work closely with governmental agencies, including, among others, DOE, the United States Department of Homeland Security, Natural Resources Canada, and Public Safety Canada.

    1.5 NERC shall strengthen and expand these functions and working relationships with the electricity sector, other Critical Infrastructure industries, governments, and government agencies throughout North America to ensure the protection of the infrastructure of the Bulk Power System.

    1.6 NERC shall coordinate with the ESCC and the Government Coordinating Council.

    1.7 NERC shall coordinate with other Critical Infrastructure sectors through active participation with the other Sector Coordinating Councils, other ISACs, and the National Infrastructure Advisory Council.

    1.8 NERC shall encourage and participate in coordinated Critical Infrastructure protection exercises, including interdependencies with other Critical Infrastructure sectors.

1.9 As part of the E-ISAC's efforts to fulfill its mission, it may issue, as circumstances warrant, written communications, referred to as All Points Bulletins (APBs), to disseminate critical security information rapidly to electricity sector asset owners and operators as security threats and attacks develop, and critical, time-sensitive security information becomes available. The E-ISAC shall share all APBs with Federal Energy Regulatory Commission staff no later than at the time of issuance.

2. Security Planning

2.1 NERC shall take a risk management approach to Critical Infrastructure protection, considering probability and severity, through identification, protection, detection, response, and recovery functions.

2.2 NERC shall consider security along-side considerations of reliability and resiliency of the Bulk Power System.

2.3 NERC shall keep abreast of the changing threat environment through collaboration with appropriate government agencies.

2.4 NERC shall develop criteria to identify critical physical and cyber assets, assess security threats, identify risk assessment methods, and assess effectiveness of physical and cyber protection measures.

2.5 NERC shall support implementation of the Critical Infrastructure Protection Standards through education and outreach.

2.6 NERC shall review and improve existing security guidelines, develop new security guidelines to meet the needs of the electricity sector, and consider whether any guidelines should be developed into Reliability Standards.

2.7 NERC shall conduct education and outreach initiatives to increase awareness of security matters and respond to the security needs of the electricity sector.

2.8 NERC shall strengthen relationships with federal, state, and provincial government agencies on Critical Infrastructure protection matters.

2.9 NERC shall maintain and endeavor to improve mechanisms for the sharing of sensitive or classified information with federal, state, and provincial government agencies on Critical Infrastructure protection matters.

2.10 NERC shall improve methods to assess the impact of a possible physical attack on the Bulk Power System and means to deter, mitigate, and respond following an attack.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment B

Proposed Revisions to ROP Section 1003
Redline

1003. Infrastructure Security Program

NERC shall participate in and, where appropriate, coordinate electric industry activities to promote Critical Infrastructure protection of the Bulk Power System in North America. NERC shall, where appropriate, take a leadership role in Critical Infrastructure protection of the electricity sector to help reduce vulnerability and improve mitigation and protection of the electricity sector's Critical Infrastructure. To accomplish these goals, NERC shall perform the following functions.

1. Electricity Information Sharing and Analysis Center (E-ISAC)

    1.1 NERC shall operate the E-ISAC on behalf of the electricity sector. In 1998, the U.S. Secretary of Energy asked NERC to serve as the information sharing and analysis center for the electricity sector, in implementation of Presidential Decision Directive 63, as part of a public/private partnership to deal with matters related to infrastructure security.

    1.2 The E-ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity sector, across interdependent sectors, and with government partners. The E-ISAC, in collaboration with the United States Department of Energy (DOE) and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

    1.3 NERC shall improve the capability of the E-ISAC to fulfill its mission.

    1.4 NERC shall work closely with governmental agencies, including, among others, DOE, the United States Department of Homeland Security, Natural Resources Canada, and Public Safety Canada.

    1.5 NERC shall strengthen and expand these functions and working relationships with the electricity sector, other Critical Infrastructure industries, governments, and government agencies throughout North America to ensure the protection of the infrastructure of the Bulk Power System.

    1.6 NERC shall coordinate with the ESCC and the Government Coordinating Council.

    1.7 NERC shall coordinate with other Critical Infrastructure sectors through active participation with the other Sector Coordinating Councils, other ISACs, and the National Infrastructure Advisory Council.

    1.8 NERC shall encourage and participate in coordinated Critical Infrastructure protection exercises, including interdependencies with other Critical Infrastructure sectors.

1.9 As part of the E-ISAC's efforts to fulfill its mission, it may issue, as circumstances warrant, written communications, referred to as All Points Bulletins (APBs), to disseminate critical security information rapidly to electricity sector asset owners and operators as security threats and attacks develop, and critical, time-sensitive security information becomes available. The E-ISAC shall share all APBs with Federal Energy Regulatory Commission staff no later than at the time of issuance.

2. Security Planning

2.1 NERC shall take a risk management approach to Critical Infrastructure protection, considering probability and severity, through identification, protection, detection, response, and recovery functions.

2.2 NERC shall consider security along-side considerations of reliability and resiliency of the Bulk Power System.

2.3 NERC shall keep abreast of the changing threat environment through collaboration with appropriate government agencies.

2.4 NERC shall develop criteria to identify critical physical and cyber assets, assess security threats, identify risk assessment methods, and assess effectiveness of physical and cyber protection measures.

2.5 NERC shall support implementation of the Critical Infrastructure Protection Standards through education and outreach.

2.6 NERC shall review and improve existing security guidelines, develop new security guidelines to meet the needs of the electricity sector, and consider whether any guidelines should be developed into Reliability Standards.

2.7 NERC shall conduct education and outreach initiatives to increase awareness of security matters and respond to the security needs of the electricity sector.

2.8 NERC shall strengthen relationships with federal, state, and provincial government agencies on Critical Infrastructure protection matters.

2.9 NERC shall maintain and endeavor to improve mechanisms for the sharing of sensitive or classified information with federal, state, and provincial government agencies on Critical Infrastructure protection matters.

2.10 NERC shall improve methods to assess the impact of a possible physical attack on the Bulk Power System and means to deter, mitigate, and respond following an attack.