NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

National Infrastructure Protection Plan Request for Comments North American Electric Reliability Corporation Response – July 8, 2013

Request for Comments Overview

The North American Electric Reliability Corporation (NERC) hereby responds to the Department of Homeland Security's (DHS) notice and request for comments on the "Review and Revision of the National Infrastructure Protection Plan (NIPP)" (Docket Number DHS-2013-0024), Fed. Reg. Vol. 78, No. 109 (June 6, 2013) at p. 34112.

NERC was certified as the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission, on July 20, 2006, pursuant to Section 215(c) of the Federal Power Act.[1] NERC operates the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) on behalf of the Electricity Sub-sector. The ES-ISAC was established in 1998, under Presidential Decision Directive 63, which defined infrastructure industries critical to our national economy and public well-being. The ES-ISAC facilitates communications between Electricity Sub-sector participants, the Federal Government, and other critical infrastructure industries (*i.e.*, information sharing).

Generally, NERC supports the existing structures identified in the NIPP and believes that the ES-ISAC and other sector information sharing and analysis centers (ISACs) work well to support these activities and should be continued. The following are NERC's specific comments on elements of Presidential Policy Directive 21 that will be included in the successor to the NIPP.

1. Identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure

NERC formalized cyber incident risk management by developing NERC critical infrastructure protection (CIP) reliability standards, which are mandatory and enforceable for certain users, owners, and operators of the Bulk Power System (BPS). NERC approaches cybersecurity through the use of a risk management framework that ensures NERC registered entities are focused on the greatest risks to BPS reliability.

NERC's mandatory CIP reliability standards provide foundational security, which in combination with the ES-ISAC alerts and notifications, provide a comprehensive approach to security and resilience of critical infrastructure.

[1] *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (2006).

Specifically, the ES-ISAC shares information and guidance with the Electricity Sub-sector concerning cybersecurity issues and events. Threat information is provided and received through a secure portal. The ES-ISAC issues alerts that provide authoritative information and coordination guidance and have been implemented and formalized across industry.

Also, NERC uses the Electricity Sub-sector Cybersecurity Risk Management Process (RMP) Guideline, a cyber-specific guidance model that employs progressive threat level action planning. The RMP was developed with the Department of Energy (DOE), the National Institute of Standards and Technology (NIST), NERC, and the sub-sector, and supports ongoing development and measurement of cybersecurity capabilities and entity risk within the sub-sector. The primary goal of this RMP guideline is to describe an RMP that is tailored to the specific needs of Electricity Sub-sector organizations. It is based on the NIST Special Publication 800-39, "Managing Information Security Risk."

NERC also works to enhance the focus on workforce development and training to improve human responses to attacks (*e.g.*, spear phishing). This activity identifies best practices to ensure the workforce understands how to identify and address threats that affect critical infrastructure.

In addition to serving as the ES-ISAC, NERC currently participates in the Electricity Sub-sector Coordinating Council (ESCC) and coordinates with the Energy Government Coordinating Council. These two structures, as identified in the NIPP, are important components to any cybersecurity framework because sector-specific planning and coordination are addressed through coordinating councils. As the NIPP states, these councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to critical infrastructure and key resources protection and work together to advance capabilities.[2]

In combination with mandatory CIP reliability standards, a comprehensive approach to risk management for cybersecurity risk management provides opportunities for public-private partnerships and increased communication to occur. NERC supports an update of the NIPP that reaffirms these existing efforts and builds on existing structures in place, such as NERC's mandatory CIP reliability standards, the ES-ISAC, the ESCC, and the RMP.

Finally, the ES-ISAC and ES-ISAC personnel have no responsibilities for the NERC Compliance Monitoring and Enforcement Program (CMEP). ES-ISAC personnel do not directly or indirectly report or convey information to the CMEP or to personnel assigned to that program about possible violations they may encounter or learn about in the course of their ES-ISAC activities. NERC has sufficient other means at its disposal to address possible violations of mandatory CIP reliability standards or an imminent threat to the reliability of the BPS.

[2] http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

2. Protocols to synchronize communication and actions within the Federal Government

Taking full advantage of the ISACs would assist in overcoming information sharing hurdles among organizations, government, and sectors. Using these existing structures provides an efficient and streamlined process for information sharing. In addition, industry requires better access to information from the government, which can be accomplished through the declassification of relevant information and increased access to government briefs. Increasing the flow of non-classified threat information from the Federal Government to entities would improve information sharing.

In addition to using the ISACs, the ESCC should remain intact and strengthened. The coordination and protected information sharing that does occur between government and industry is critical, and must continue.

NERC also advises that the Critical Infrastructure Partnership Advisory Council framework remain intact and effectively utilized, as appropriate, for coordinating council proceedings. All of the coordinating councils use this authority to protect sensitive conversations, and since it is an existing structure at DHS, this group would address the need to maintain the framework for sensitive conversations.

3. A metrics process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure

NERC and the Electricity Sub-sector are unique among critical infrastructure sectors as mandatory CIP reliability standards, developed through a consensus-based process, already exist as a part of its full body of comprehensive reliability standards. NERC reliability standards define the requirements for planning and operating the North American BPS, and are developed using a collaborative, structured and transparent results-based approach, that focuses on performance, risk management, and entity capabilities.

Reliability standards are generally written as performance standards; that is, they prescribe an end-state or goal that can be measured, and attempt to avoid specification of particular technologies and methods for attaining desired performance outcomes. In addition to the CIP reliability standards, NERC has also developed operational standards for the sub-sector, including the Emergency Operations Planning standards that address operational resilience through mandated backup and recovery objectives.

In addition, the ES-ISAC provides key tools for the Electricity Sub-sector to address new threats and vulnerabilities. ES-ISAC activities support risk-informed standards development and application. The ES-ISAC also conducts Cyber Risk Preparedness Assessments (CRPA) of NERC registered entities, assessing entity capability and response to cybersecurity challenges.

While CIP reliability standards are specific to the Electricity Sub-sector, many of the concepts provide baseline security measures that may potentially inform approaches to real-time process control networks and systems in other sectors as well.

The new CIP reliability standards (CIP Version 5) include NIST framework concepts such as:

- Ensure that all Bulk Electric System (BES) cyber systems associated with the BPS, based on their functions, receive some level of protection;
- Use a tiered approach to security controls, which specifies the level of protection appropriate for systems based on their importance to the reliable operation of the BPS;
- Tailor protection to the mission and operating environment of the cyber systems subject to protection;
- Define the concept of the BES cyber system; and
- Include "Assess" and "Monitor" steps by adding requirement language for "Identifying, Assessing, and Correcting" deficiencies in controls as part of the requirements' expected performance.

As part of a registered entity's continuity of operations plans, many organizations will identify critical functions necessary to deliver electric power and restore systems. Additionally, organizations with mature cybersecurity programs will develop recovery time objectives for incident response and recovery operations, and incorporate these objectives into their plans and procedures. During exercises, organizations can test these recovery time objectives to see if restoration and recovery plans are effective. During expert assessments, entities already have the opportunity to apply elements of NERC's CRPA and integrated ES-C2M2 content, which assists entities in identifying and considering gaps and opportunities for resilience enhancement activity.

4. Description of functional relationships within DHS and across the Federal Government related to critical infrastructure and resilience

NERC participates in, and provides leadership to, several government-industry partnership initiatives and organizations. NERC believes the existing structures identified in the NIPP work well to support these activities and should be continued as long NERC continues its role in this effort. Some of the partnership initiatives NERC is engaged in include:

- Partnership for Critical Infrastructure Security, the senior-most policy coordination group between public and private sector organizations comprised of the chairs or co-chairs of all 16 critical infrastructure and key resources sectors and their Government Coordinating Council counterparts;

- Cross-Sector Cyber Security Working Group, which was established to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services;
- Industrial Control Systems Joint Working Group, which is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, and coordinated efforts to develop better vendor focus on security needs for industrial control systems; and
- Energy Security Public-Private Partnership, a CIPAC joint working group composed of DOE, DHS, the Department of Defense (DOD), and key sector stakeholders to address DOD Defense Critical Infrastructure Program matters in a manner sensitive to the Federal Advisory Committee Act and security classification concerns.

NERC also collaborates with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

In addition, NERC participates in activities such as the DHS National Level Exercise series and various cybersecurity forums and briefings with Canadian government agencies, as well as the White House-initiated, DOE led Electricity Sub-sector Cybersecurity Capability Maturity Model (ES-C2M2). ES-C2M2 was created to support ongoing development and measurement of cybersecurity capabilities within the Electricity Sub-sector through the following four objectives:

- Strengthen cybersecurity capabilities in the Electricity Sub-sector;
- Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities;
- Share knowledge, best practices, and relevant references within the sub-sector as a means to improve cybersecurity capabilities;
- Enable utilities to prioritize actions and investments to improve cybersecurity.

5. Changes to sector partnerships resulting from the evaluation of the existing public-private partnership model

In accordance with section 215 of the Federal Power Act, which was added by the United States Energy Policy Act of 2005, NERC has strengthened working relationships with the Electricity Sub-sector and government to ensure the protection of BPS infrastructure. Section 215 made compliance with reliability standards mandatory and enforceable for users, owners, and operators of the BPS within the United States.

Sector Specific Agencies (SSA) are government departments that facilitate the unified public and private sector effort to improve sector resilience. The SSA should work closely with the Government Coordinating Council and Sector Coordinating Council to facilitate support for the ISACs. Additionally, the Government Coordinating Council and Sector Coordinating Council with SSA support should fully address executive alignment of priorities towards the following:

- Improving timely and actionable threat information sharing;
- Defining sector partner organizations' roles and responsibilities;
- Clarifying departmental and corporate resourcing and organizational structure and policy for enhanced security dialogue and reporting;
- Providing programmatic and resource support for improved cross-sector information sharing using the sector ISACs;
- Emphasizing utilization and improvement of Unified Coordination Group (UGC) structures and processes;
- Supporting sector analysis and understanding, as well as capability maturation encouragement; and
- Achieving leadership consensus across public-private partnerships, which drives emerging policy, implementation guidance, resource adequacy, and role definition.

The current threat landscape is dynamic in nature. NERC reliability standards provide a foundation of security and the ES-ISAC provides actionable intelligence on vulnerabilities to the Electricity Sub-sector.

6. Consider sector dependencies on energy and communications systems and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems

Critical sectors such as information technology, communications, and transportation may affect industrial control systems, energy market systems, energy management systems, and various energy generation, transmission, and distribution systems. Sector analytic and communications/coordination tools may also be affected by interdependent critical sectors. As such, the revised NIPP must be flexible enough that common elements can reach across sectors and prevent a "siloed" approach to critical infrastructure protection, but still ensure that the individual sectors maintain control of their own infrastructures. Sector specific updates to information sharing tools and mechanisms can assist with addressing sector dependencies. NERC has evaluated some of these concerns through task force reports, including a report on information sharing[3] and severe impact resiliency,[4] which identified findings that provided a

[3] http://www.nerc.com/comm/CIPC/Electricity%20Sector%20Information%20Sharing%20Task%20For1/Electricity%20Sector%20Information%20Sharing%20Task%20Force%20(ESISTF)%20Draft%20Report.pdf.

[4] http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

comprehensive focus on pre-event and mitigation steps. The electric industry has significant experience with mitigation and event response due to storm response and mutual assistance programs. This knowledge assists in pre-event and mitigation measures associated with cross-sector dependencies. Industry applies this knowledge to security and resilience efforts, recognizing a continuous need for education, training, and the application of lessons learned.

The coordinating councils serve an important role in providing cross-sector information, but additional sector coordination could significantly reduce impact exposure in other critical sectors, assets, and missions. NERC provides strong support for the coordinating councils, ISACs, and the Cyber Unified Coordination Group as essential foundational elements of the NIPP and seeks to continue that role.

Also, conducting regular exercises to test response measures and identify vulnerabilities can assist with individual sector coordination efforts and can be expanded on to include other sectors with interconnected vulnerabilities. NERC conducts industry security exercises, participates in national level exercises, and sponsors security conferences and webinars. NERC has also provided subject matter expertise to industry products, resulting in refined industry response plans. Finally, NERC supports regional catastrophe planning and exercise activity.