Statement of James B. Robb
President and CEO, North American Electric Reliability Corporation
FERC/DOE Security Investments for Energy Infrastructure Technical Conference
Docket No. AD19-12-000
March 28, 2019

The Federal Energy Regulatory Commission (FERC or Commission) and U.S. Department of Energy (DOE) ask important questions concerning the need for security investments that go beyond those required by mandatory reliability standards. The security challenge is continuously evolving and growing in complexity. Reliability and security are intertwined when it comes to critical infrastructure protection. The North American Electric Reliability Corporation (NERC) employs a holistic approach to security, with standards as a universal foundation, timely and actionable information exchange and analysis by the Electricity Information Sharing and Analysis Center (E-ISAC), sharing of best practices, cross-sector collaboration, and effective partnerships with government. NERC's work with FERC, DOE, and the Electricity Subsector Coordinating Council (ESCC) assure a reliable and secure grid against ever increasing challenges.

At no point in its history has the electricity industry faced so many challenges simultaneously. Driven by new technology, public policies, and changing consumer preferences, the industry is undergoing a fundamental and rapid evolution. These changes are happening at the same time that the value of electricity is increasing with continued electrification. Over 340 million people in North America are increasingly dependent on safe and reliable electricity.

The shifting resource mix is creating challenges and opportunities. Because this evolution is driving a new business model, incentives to improve security should be informed by the reality that industry is also making major investments in new generation and energy delivery. This is occurring as industry is implementing the current version of the critical infrastructure protection standards, including requirements for cyber and physical security, supply chain management, and, in the future, broader cyber incident reporting. In addition, companies will be investing to protect their systems from naturally occurring geomagnetic events.

Today's conversation on incentives for security investments can ensure that industry is allocating resources efficiently and effectively. Just as NERC provides a risk-based model that focuses resources on areas of greatest reliability risk, security incentives should be structured to align with the highest priorities. Incentives should have sufficient breadth and flexibility to accommodate entities of varying size and ownership type. Broad, active data sharing by all entities is an essential best practice for all entities. Accordingly, the Commission may seek to examine incentives to facilitate participation in the Cybersecurity Risk Information Sharing Program and other data sharing programs. Since it is easier to

protect a system that is designed with security in mind, the Commission could also consider measures to encourage investment in systems that narrow the attack surface.

Even in the face of many challenges, it is important to stress that industry is strongly committed to security. Among the critical infrastructure sectors, electricity leads the nation for its culture of security, sophistication, and partnerships. While our work is never done, we should recognize this success.

This statement further discusses (1) the role, services, and products of the E-ISAC; (2) cybersecurity threats and trends; (3) interdependencies among energy infrastructure from a security perspective; and (4) designing a more secure system.

Electricity Information Sharing and Analysis Center
Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance requires constant situational awareness, real time communication, and prompt emergency response capabilities. The E-ISAC provides these services and supports these industry capabilities. The E-ISAC also runs NERC's GridEx program and other learning opportunities for industry.

The mission of the E-ISAC is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and analysis in a timely, credible, actionable manner with asset owners and operators across the continent.

Operated by NERC, and working in collaboration with the DOE and the ESCC, the E-ISAC is the central information sharing hub for the electricity sector. The E-ISAC uses a secure portal as the primary means for communicating with its over 1,025 electricity industry member organizations, and the number continues to grow. The portal was revamped in 2017 and is constantly undergoing further upgrades to enhance the user experience. The new portal functions, plus greater outreach with key industry stakeholder groups through our Industry Engagement Program (IEP), has improved bi-directional information sharing and allows members greater access to more information.

E-ISAC services enable industry to defend against and respond to cyber and physical security threats, vulnerabilities, and incidents through the exchange of timely, actionable information. In addition to coordination with DOE and FERC's Office of Energy Infrastructure Security, the E-ISAC promotes cross-sector coordination through work with the U.S. Department of Homeland Security (DHS) and other agencies and ISACs. In particular, to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC continues to expand its partnership with the Downstream Natural Gas ISAC (DNG-ISAC). In the past year, the E-ISAC added additional partnerships with other interdependent sectors, including the Water-ISAC and the Multi-State ISAC with the goal providing electricity sector context to water and waste-water operators, as well as state and local government. Security is a global priority, and because NERC is an international organization, the E-ISAC works with Natural Resources Canada, Public Safety Canada, and the recently established Canadian Centre for Cyber Security to provide cross-border outreach and collaboration. In October 2018, NERC announced a trilateral memorandum of understanding among the E-ISAC, the Japan Electricity ISAC and the European Energy ISAC with the intention of expanding sources of information and opportunities for analysis with partners who face similar adversarial threats. As the E-ISAC moves to 24/7 watch operations, these

international partnerships will provide valuable context and awareness of emerging threats for overnight analysts to share with North American grid operators.

Cybersecurity Risk Information Sharing Program (CRISP)

Managed by the E-ISAC and in partnership with DOE, CRISP uses innovative technology to look for adversary activity in internet traffic, and leverages DOE and its National Laboratory System's analytical capability. CRISP provides timely bi-directional sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP companies cover over 75 percent of U.S. customers. CRISP information is shared in a secure fashion through the E-ISAC Portal, and allows non-CRISP member companies to benefit from the shared indicators and threat actor activity captured by the program. CRISP information also supports the development of situational awareness to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources. In addition to CRISP, the E-ISAC is pursuing cyber automated information sharing systems as well as a malware analysis repository and threat information exchange to provide for more advanced information sharing capabilities. Under DOE's leadership, CRISP is expanding to at least 30 more energy utilities that may not have the resources to join the program. By leveraging the existing CRISP public-private model, DOE is incentivizing smaller, but still very important, companies to join this effective data sharing initiative. DOE is also piloting a program to provide similar protections to industrial control systems, called Cybersecurity for Operational Technology Environment (CyOTE), which would be a benefit for national security.

NERC Alerts, Critical Broadcasts, and Briefings

In addition to the secure portal, the E-ISAC shares information through a number of forums to increase awareness of threats, and to recommend mitigation. When there is a significant security concern, NERC and the E-ISAC communicate with the electricity industry via two distinct platforms.

NERC Alerts provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Alerts are divided into three levels:

- Level One – Industry Advisory: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Level Two – Recommendation to Industry: Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the alert.
- Level Three – Essential Action: Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the alert.

NERC determines the appropriate alert notification based on risk to the Bulk Power System (BPS). Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its compliance registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and

operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., balancing authorities, transmission operators, generation owners, etc.).

Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has issued 46 security-related Alerts, 41 of which were cyber-related (41 Industry Advisories and 5 Recommendations to Industry). Those alerts covered items such as sabotage events, pandemic, and heightened awareness and reporting guidance of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the 2015 cyber-attack in Ukraine and another concerning distributed denial of service attacks leveraging compromised Internet of Things[1] devices. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

In addition to NERC alerts, the E-ISAC uses the Critical Broadcast Program (CBP). This program launched in 2018 to rapidly share information with members, either through conference calls or "All-Points Bulletins" to stand out from routine portal postings and notifications. The CBP leverages E-ISAC staff and stakeholder expertise to obtain and share the best available information and potential mitigation strategies to address developing security threats and events in a timely manner. Additional information is then shared through the E-ISAC portal and other means, as necessary. The E-ISAC used this capability four times in 2018: on February 7, where 1,208 individuals joined the call; February 20 with 960 individuals; November 29, with 524 participants; and December 20, where over 1,284 individuals from the electricity and oil and natural gas sub-sectors joined the call.

The E-ISAC also hosts regular monthly threat briefings, unclassified threat workshops, participates in government-hosted classified forums for its members, and allows asset owners and operators to interact with our analysts and each other to share trend analysis and context on common threats to the electricity sector. In addition to the regularly hosted events, the E-ISAC conducted seven sessions of the IEP in 2018, which are three-day sessions where industry members visit the E-ISAC to see firsthand how the E-ISAC operates on a daily basis. These activities allow members to discuss emerging threats, learn from security experts, and provide feedback directly to the E-ISAC—which help improve E-ISAC's products and services, and builds trust directly with stakeholders.

GridEx
Consistent with our mission to promote a strong learning environment, NERC hosts an every other year grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure designed to overwhelm even the most prepared organizations. GridEx is the largest geographically distributed grid security exercise for the electricity sector. It consists of a two-day distributed play exercise and a separate executive tabletop session. GridEx enables participants to:

- Exercise incident response plans;
- Expand local and regional response;

---

[1] The Internet of Things (IoT) refers to devices and sensors connected to the Internet such as security cameras, alarm systems, printers, or light switches. IoT devices typically use default passwords and are highly vulnerable to subversion by threat actors.

- Engage critical interdependencies;
- Increase supply chain participation;
- Improve communication; and,
- Gather lessons learned.

In 2017, 6,500 individuals and 450 organizations participated in GridEx IV, including industry, law enforcement, and government agencies. The executive tabletop included 42 participants from a cross-section of industry executives and senior officials from federal and state governments. Participating organizations are encouraged to identify their own lessons learned and share them with NERC. NERC uses this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. We are deep into planning for GridEx V which will be conducted on November 13-14, 2019.

GridSecCon
Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together hundreds of cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry. While the specific agenda varies from year to year, general objectives include:

- Promoting reliability of the BPS through training and industry education;
- Delivering cutting-edge discussions on security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and
- Informing industry with discussions on security best practices, reliability concerns, risk mitigation, and cyber and physical security threat awareness.

Cyber Threats and Trends
These engagements and analytical capabilities have increased the E-ISAC's insight into threats to the grid. This greater insight has translated into more security products for industry, as well as more member-originated information submitted to the E-ISAC and more sharing. In 2018, more than 300 cyber bulletins and more than 200 physical bulletins were posted to the portal. The E-ISAC also posts bulletins based on information obtained from government partners and trusted open source partners, and we thank our government partners at DOE, DHS, and FBI for continuing to produce these valuable products.

Looking at the trend analysis of those bulletins, the major cyber and physical security trends of 2018 included: adversary advanced persistent threat (APT) activity, phishing, malware, gunfire at electric infrastructure, and theft. From a cyber perspective, nation-state activity against the energy sector is extremely concerning, and we are very grateful for government shares on adversaries' latest tactics, techniques, and procedures. While many physical security threats remain similar from year-to-year, the threat from activist groups continue to evolve as they become more capable.

In 2018, many familiar malware families such as Shamoon and GreyEnergy—the successor to BlackEnergy—saw new variants, while other frameworks like VPNFilter first appeared. In the case of

VPNFilter, the E-ISAC leveraged its partnership with an industrial control system vendor to quickly dispel concerns regarding the Modbus module's capabilities. The threat, however, is clear: advanced attackers continue to develop highly modular tools with the ability to greatly impact a targeted system.

As the E-ISAC looks to the future, we anticipate certain trends:

Credential harvesting: Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular, because it helps evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.

Exploitation of the trust relationship between targeted organizations and their business partners: Recent incidents have demonstrated that nation-state adversaries are targeting the electric sector and other industries by compromising the networks of third parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack, and increases the success rate of tactics used to initially compromise the intended target.

Network device targeting: From the high profile reports on VPNFilter to the state-sponsored actors targeting network devices discussed in United States, switches and routers located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet, and exist to allow controlled access to the internal network, they will most likely continue to be a target of reconnaissance.

Use of native tools: Adversaries will likely continue to use tools and capabilities already present on a compromised network – such as PowerShell or Windows Management Infrastructure (WMI) – to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

Energy Infrastructure Interdependencies
The Commission poses an important question about interdependencies among energy infrastructure. In November 2017, NERC published the Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System Report.[2] In the Report, NERC makes numerous recommendations for assessing disruptions to natural gas infrastructure and related impacts to the reliable operation of the Bulk Electric System (BES). The report recommends that federal regulators and agencies work with natural gas pipeline operators and evaluate potential cyber and physical security vulnerabilities on the natural gas system's infrastructure and control facilities. Policy makers should ensure gas infrastructure is as secure from cyber and physical threats as the grid it supplies. Additionally, gas industry regulators should be engaged to establish cyber security standards that match those of the NERC reliability standards.

---

[2] *See report:* https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf

Designing a More Secure System

The transforming electric grid presents opportunity to incorporate security into system design-basis during the planning stage, rather than as a retrofit or afterthought. Specifically, systems should be designed to narrow the cyber and physical attack surfaces, with built-in resilience components that support withstand, degradation and recovery timeframes. New principles, processes, and procedures in the planning, operating, and protection disciplines can and should be tightly integrated into the ongoing transformation of the BPS. NERC's Reliability Issues Steering Committee recognizes this need in its latest report, which identifies specific activities over a one- to five-year timeframe and beyond.[3] Incentives could play a role in supporting investments in this area.

Conclusion

Reliability is NERC's mission, and grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of complementary strategies. Our partnerships are critical to the electricity sub-sector's priority for security. Mandatory CIP standards provide a universal foundation for security and is a shared priority with FERC and industry. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong public private partnerships are key to successful information sharing within the electricity sector and across sectors. NERC remains keenly focused on our mission to assure reliability of the BPS.

---

[3] *See report:* https://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO-Reliability-_Risk_Priorities-Report_Board_Accepted_February_2018.pdf