NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Reliability Technical Conference

Panel IV: Grid Security

Remarks of Marcus Sachs, Senior Vice President and Chief Security Officer
North American Electric Reliability Corporation
June 22, 2017

Introduction

Good afternoon. My name is Marc Sachs and I am the Senior Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC). Thank you for the opportunity to appear before the Commission to discuss grid security and the work NERC and the Electricity Information Sharing and Analysis Center (E-ISAC) are doing to mitigate potential impacts on the bulk power system (BPS).

Assessing security risks and their potential impact is a complex endeavor facing industries around the world. The security landscape is dynamic, requiring constant vigilance and agility. The risk and threats to security are evolving due to geopolitical tensions and changing societal trends. In addition, the adversary is becoming more sophisticated and we are seeing more state-sponsored activity. Assessing security risks impacting the BPS is equally challenging; however, NERC and its E-ISAC understand both the BPS and the complexities of security, and we have taken significant steps to address security across the electricity industry. From the E-ISAC's perspective, we are achieving security objectives through a range of strategies, including building out the E-ISAC's cyber and physical security analysis teams and capabilities, and increasing our information sharing and member engagement activities. I am pleased to report on our progress to date and our strategic focus on the future.

NERC addresses cyber risk through a variety of regulatory and non-regulatory means. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections. However, due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's E-ISAC serves as the information sharing conduit between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to maintain "ground truth" during rapidly evolving security events. Together, mandatory standards, coupled with effective mechanisms to share information, provide robust and agile tools to protect the BPS. In addition, NERC works closely with the Electricity Subsector Coordinating Council (ESCC) to further the public-private partnership that is so important to addressing security.

State of Reliability 2017 includes a report on the state of grid security. It details the evolving nature of risk and outlines our progress in measuring and understanding it.[1] Specifically, the data NERC received in 2016

[1] *State of Reliability 2017*.

from OE-417s[2] and EOP-004s[3] show low numbers of cyber penetrations of grid operating systems in North America and few reports of physical intrusions.[4] These low numbers indicate that NERC's efforts with industry have been successful in isolating and protecting operational systems from various adversaries. These numbers also indicate that the electricity industry's record of breaches is much lower than many other sectors, including government agencies that have been victims of numerous data breaches. Overall, the electricity industry is doing well in identifying and mitigating risks to the BPS.

Beyond Standards and Compliance

The E-ISAC's mission is to be a leading and trusted source that analyzes and shares electricity industry security information. The E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry across interdependent sectors and with government partners.

Our analysts have tools available to help them understand the latest cyber threats. Two of the E-ISAC's analytical capabilities, such as the Cybersecurity Risk Information Sharing Program (CRISP) and the Cyber Automated Information Sharing System (CAISS) offer options outside of standards to calculate risk indices based on the number of cyber incidents discovered.

In addition to these analytical capabilities, the E-ISAC engages in a range of information sharing activities that help further mitigate potential impacts on BPS operations. For example, the E-ISAC convenes subject matter experts at our annual Grid Security Conference (GridSecCon) to examine issues impacting the electricity industry. Also, our biennial Grid Security Exercise (GridEx) provides an opportunity for industry to apply crisis response and recovery plans around simulated attacks to critical electric infrastructure. Finally, we take what we have learned and conduct regular outreach with industry asset owners and operators (AOO) to promote a learning environment and strong culture of security.

Most of the E-ISAC's communications with electricity industry members are via an Internet portal that was significantly upgraded at the end of 2015, and is currently undergoing a transformation from a portal to a portal-platform. The new platform will enhance bidirectional information sharing and allow members greater access to more information. This enhancement is part of the E-ISAC Long-Term Strategic Plan, which builds on recommendations from the ESCC, and discusses improvements needed in 2017 to address current threats.

Increased physical security and cyber security information sharing will further enhance the volume and sophistication of the E-ISAC's analysis capabilities. Robust data collection over time helps identify important trends and patterns. By providing unique insight and analysis on physical and cyber security risks, the

[2] Form OE-417 is the Electric Emergency Incident and Disturbance Report, which collects information on electric incidents and emergencies. The Department of Energy uses the information to fulfill its overall national security and other energy emergency management responsibilities, as well as for analytical purposes. NERC also accepts this form as part of industry EOP reporting requirement.
[3] EOP-004 is a NERC form that Responsible Entities use for reporting. The forms are to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.
[4] See Appendix G in *State of Reliability 2017* for the security metrics.

E-ISAC's aim is to add value for its members and assist with overall risk reduction across the Electric Reliability Organization (ERO) Enterprise.

Analysis Capabilities

Over the past several years, the E-ISAC has enhanced its analysis capabilities by building out our cyber and physical security analysis teams and adopting new tools and programs.

The cyber analysis team provides analysis on information shared to produce actionable indicators and builds the cyber "big picture" that is shared with members. This includes vetting information shared by government and cross-sector partners for validity while also explaining how certain indicators would apply to the sector. The physical security analysis team receives both mandatory reporting and member direct report contacts, and performs detailed analysis on all physical security events.

The analysts have access to tools and programs that help them understand threats and assess risk. These combined capabilities enable the E-ISAC to keep industry informed about potential threats to the BPS and the sector as a whole, and help industry mitigate these threats. Two main cyber programs are CRISP and CAISS.

CRISP is a public-private partnership, cofounded by the Department of Energy (DOE) and NERC, and managed by the E-ISAC, that facilitates the exchange of detailed cyber security information among industry (i.e., E-ISAC, DOE, and Pacific Northwest National Laboratory). The purpose of CRISP is to collaborate with industry partners to facilitate the timely bidirectional sharing of unclassified and classified threat information, thereby enabling owners and operators to better protect their networks from sophisticated cyber threats. CRISP participant companies serve approximately 75 percent of electricity consumers in the United States. CRISP information also helps support development of situational awareness tools to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

CAISS is a NERC program, in collaboration with the DOE and the national laboratories, to capture operational traffic, in addition to the large data sets of information flowing from the corporate or business systems. Once CAISS—which is currently a pilot program—becomes more widespread, it will allow indicators of compromise (IOC) that may be seen on enterprise information technology systems via CRISP to be compared to any potential intrusions or malicious data collected from control systems, further refining risk metrics to grid operations.

Cyber Threats

These 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. In 2016, the E-ISAC saw 241 cyber bulletins posted to the E-ISAC portal.[5] Of the 241 cyber bulletins, 210 were posted based on information provided by members or posted by members

[5] Bulletins describe physical and cyber security incidents and provide timely, relevant, and actionable information of broad interest to the electricity industry.

themselves. This trend is consistent with the 218 cyber bulletins in 2015. The E-ISAC expects this number to increase in 2017 as member participation increases. The E-ISAC also posted several bulletins based on information obtained from government partners and trusted open source partners. Like 2015, the second quarter of 2016 saw the most portal posts based on information provided by members.

For 2016, just under half of the reports from members involved phishing incidents. Other important trends and analysis conducted throughout the year focused on the Dridex campaign, ransomware, and the Internet of Things (IoT). The E-ISAC also monitored several important cyber events in 2016, including malicious cyber activities by the Russians and a power outage in Ukraine.

Several key topics and takeaways from the analysis of reports in 2016 include the following:

Ukraine: Cyber attacks on three distribution utilities in Ukraine on December 23, 2015, garnered significant attention. These utilities were attacked through a variety of means, including spear phishing, credential harvesting and lateral movement, unauthorized remote access, telephony denial-of-service, and sustaining persistent access. In February 2016, NERC's E-ISAC provided subject matter expertise to develop a non-public NERC alert, *Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced by Recent International Events*, which shared techniques observed in the Ukraine cyber attacks. Most of these same tactics and techniques were used in a subsequent series of attacks against Ukraine in December 2016, when Ukraine's state-owned national power company, Ukrenergo, experienced an outage at an electrical substation in the capital city of Kyiv. Service was restored as a result of manual operator intervention. Researchers confirmed that the outage was the result of a cyber attack that occurred during the end of a protracted campaign.

In addition to the 2016 NERC alert, the E-ISAC worked with the SANS Institute to publish a Ukraine Defense Use Case (DUC).[6] This 29-page report "summarizes important learning points and presents several mitigation ideas based on publicly available information on Industrial Control Systems (ICS) incidents in Ukraine."

The techniques used against Ukraine have several options for remediation and prevention. NERC, through standards and compliance; and the E-ISAC, through information sharing, industry collaboration, and publications like the NERC alert and DUC; often stresses and shares these remediation and prevention tips with the electricity industry.

The events in Ukraine underscore the importance of grid security and provide a real-world example of consequences of a cyber attack on the electrical grid. The events abroad also highlight the importance of user training and information sharing in order to prevent a similar attack on the North American power grid. Similar tactics are woven into NERC's GridEx series.

[6] "Analysis of the Cyber Attack on the Ukrainian Power Grid."

Phishing: In 2016, over 40 percent of cyber bulletins posted were about phishing. This trend is consistent with what the E-ISAC observed in 2015. These phishing emails contained information relating to the Dridex campaign, html credential harvesting, Gh0st RAT, Locky, typosquatting, whaling, and vawtrak attempts.

Ransomware: Since the beginning of 2016, E-ISAC reporting and media coverage pointed to a significant increase in ransomware-specific cyber extortion activity. Ransomware is a special class of disruptive, malicious software designed to deny access to data and files until the victim meets payment demands. Once compromised, the victim may have to restore systems from back-up tapes or pay the ransom with the hope of regaining access to the data and files. In response to the prevalence of ransomware across all critical sectors and its destructive capabilities, the E-ISAC provided subject matter expertise in a NERC Alert that was issued in June 2016.[7] The E-ISAC also released a detailed assessment in May 2016 outlining the evolution of ransomware tactics.

Internet of Things (IoT): Serious concerns surround the security of devices designed to be used as part of the IoT. Cyber security practitioners generally agree that most IoT devices connected to the Internet are likely to be a target because they generally do not have security as an important part of their design process. Due to the highly interconnected and unauthenticated state of the IoT, the lack of sufficient security design in IoT products and toys can be leveraged against critical systems accessible from the internet.

The use of a large number of IoT devices can be harnessed from all areas of the Internet rather than a small number of networks. This massive scale of the IoT devices has successfully generated attack throughput rates on the order of several hundred megabits-per-second to one terabit-per-second (tbps) or more.

The October 21, 2016, distributed denial-of-service (DDoS) attack against the Dyn-managed domain name system (DNS) infrastructure resulted in 1.2 tbps of network throughput (also referred to as bandwidth) being used against the DNS address provider's infrastructure. Malware, such as Mirai, will continue to grow as the overall throughput of internet providers' infrastructure will be the ultimate limiting factor.

A non-public Level 2 NERC Alert, published on October 11, 2016, addressed issues with IoT devices that are connected to the public Internet. In conjunction with the alert, on October 24, 2016, the E-ISAC released its *Internet of Things DDoS White Paper*.[8]

GRIZZLY STEPPE: On December 29, 2016, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a Joint Analysis Report (JAR) titled, "GRIZZLY STEPPE - Russian Malicious Cyber Activity[9]," that provided details of the tools used by Russian intelligence services to compromise and exploit networks and endpoints associated with a range of U.S. government, political, and private sector entities. The JAR also included recommended mitigations and information on how to report such incidents to the U.S. government. The E-ISAC analyzed the IOC provided by government intelligence for potential malicious network traffic that may affect the electricity industry. This cyber security finding

[7] "Industry Advisory - Ransomware Extortion Poses Increasing Risk".
[8] "Internet of Things DDoS White Paper" *at* www.eisac.com.
[9] "GRIZZLY STEPPE - Russian Malicious Cyber Activity".

demonstrates the effectiveness of successful information sharing partnerships between industry and government.

Burlington Electric Department received the JAR from DHS. Upon a scan of Burlington's system, the utility found a potentially compromised laptop. The utility conducted further analysis and investigation, determining the laptop had not been connected to the grid. Based on information currently available, the E-ISAC believes that neither the electricity industry nor this particular utility were targeted by this cyber attack. The information points to this activity as part of a broader, untargeted campaign searching for vulnerable computers to exploit. Both the wide range in age of indicators in question and the fact that addresses belonged to content providers, cloud computing providers, and internet service providers, in addition to private companies and individuals, made this activity difficult to connect to a particular actor.

Information Sharing and Member Engagement Activities

In addition to building out our analysis capabilities, the E-ISAC has increased efforts to improve information sharing and engage with industry. The E-ISAC either leads or participates in different activities that help us better understand security risks and provide members with security information and mitigation strategies.

GridEx: NERC conducted its third biennial grid security and emergency response exercise, GridEx III, on November 18-19, 2015. NERC's mission is to assure the reliability of the BPS, and GridEx III provided an opportunity for industry and other stakeholders to respond to simulated cyber and physical attacks affecting the reliable operation of the grid. Led by the E-ISAC, GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate executive tabletop on the second day. More than 4,400 individuals from 364 organizations across North America participated in GridEx III, including industry, law enforcement, and government agencies.

In March 2016, the E-ISAC released three reports (one available to the public and two restricted to industry and government stakeholders) regarding the lessons learned on GridEx III. The reports summarize the exercise and provide recommendations that the E-ISAC has integrated into its internal crisis action plan and standard operating procedures.[10] In addition, the ESCC has adopted many of the recommendations into its playbook and used the GridEx III exercise to spur action on cyber mutual assistance, increase spares of critical equipment, and provide cross-sector support during crisis situations. Finally, all participating organizations were able to improve internal and external communications and relationships with important stakeholders and exercise crisis response procedures against an advanced attack scenario that identified potential gaps and improvements to improve security, resilience, and reliability.

GridEx IV will be held November 15-16, 2017. Over 168 industry organizations have signed up to participate in distributed play across North America, already surpassing GridEx III in 2015. Similar to GridEx III, GridEx IV will include an executive tabletop session. GridEx IV objectives include: exercising incident response plans; expanding local, state, and regional response; engaging critical interdependencies; improving communication; gathering lessons learned; and engaging senior leadership.

[10] GridEx III Report.

GridSecCon: The E-ISAC convenes GridSecCon on an annual basis. In 2016, this assembly brought together over 400 electricity cyber and physical security professionals. GridSecCon 2016 provided free training on physical and cyber security issues and technologies, such as Ukraine, Grassmarlin, and Cyber Attack Defense Training Exercise for the Grid. The conference included speaker sessions discussing industry's work with government partners, space weather, hunting and killing on networks, and advanced research and development in the industry. GridSecCon 2017 will take place in St. Paul, MN, from October 17-20.

E-ISAC Monthly Briefing Series Update: The E-ISAC continues to host its monthly briefing series for AOOs, covering timely, CIP topics for participants. The briefings involved federal and technical partners, including DHS staff from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Office of Intelligence and Analysis, and the National Cybersecurity and Communications Integration Center (NCCIC), as well as FireEye and iSIGHT Partners. The monthly briefing series also includes special guest presentations.

Participation in the monthly briefings during 2016 ranged from 180 to over 400 attendees. This was the first full year that the series included a physical security section (added April 2015), and full replays were available for member download (added December 2015). Based on polling feedback, 70 to 96 percent of attendees consider the meetings to be of "Considerable Value" or "Great Value." The E-ISAC will continue to encourage industry to share security best practices and lessons learned on topics relevant to the industry by inviting more industry AOOs as guest presenters.

E-ISAC Unclassified Threat Workshop Series: As a result of planning and discussions with representatives from the ESCC, the E-ISAC has started hosting unclassified threat workshops biannually. These threat workshops bring together security experts from government and industry to discuss threats facing the electricity industry. The discussions include a focus on past threats, incidents and lessons learned, current threats that may impact industry, or views on emerging threats. The E-ISAC held its first threat workshop on December 6, 2016, in Washington, DC; the second workshop was on June 20, 2017, in Irwindale, CA.

To maximize information sharing with AOOs, the workshops include discussions between presenters and attendees during each briefing with E-ISAC analysis of the topics raised and dedicate time to industry discussion after the briefings. These discussions and added analysis by the E-ISAC better enable AOOs to mitigate threats and incorporate best practices.

Cross-sector Activities: The E-ISAC engages with the government at all levels, including international, federal, state, local, territorial, tribal, and provincial governments. It is also includes close international allies with critical infrastructure protection sector partners and other ISACs.

During 2016, the E-ISAC's federal partners were active in response to *Presidential Policy Directive 41: United States Cyber Incident Coordination* and created projects covering cyber mutual assistance, high profile exercises, cyber incident response plans, learning opportunities for the E-ISAC staff, and power outage incident technical reference products.[11] The E-ISAC worked closely with our federal partners in support of their activities and provided feedback where appropriate, such as with the recently updated National Cyber

[11] Presidential Policy Directive/PPD-41.

Incident Response Plan (NCIRP).[12] The E-ISAC has also maintained participation with the NCCIC, the National Integration Center, and the National Operations Center.

Through the National Council of ISACs (NCI), the E-ISAC is able to collaborate with all critical infrastructure-specific ISACs. The E-ISAC assisted the NCI in establishing new information sharing procedures and collaborative analytical approaches. This partnership helped lead to additional threat briefing opportunities and increased information sharing. Furthermore, this partnership allowed the E-ISAC to provide additional insight and analysis on key topics, such as the Ukraine events and the IoT emerging issue.

Security Metrics

State of Reliability 2017 marks the third year the report included a focus on security performance metrics based largely on data collected by NERC's E-ISAC and reviewed by a working group within NERC's Critical Infrastructure Protection Committee (CIPC). These metrics help provide answers to basic questions often asked by industry executives and senior managers, such as the following:

- How often do physical and cyber security incidents occur?
- To what extent do these reported incidents cause a loss of customer load?
- What is the extent of security information-sharing across the industry?
- Are cyber security vulnerabilities increasing?

For several years, NERC and the electricity industry have taken actions to address cyber and physical security risks to the BPS as a result of potential and real threats, vulnerabilities, and events. These security metrics complement other NERC reliability performance metrics by defining lagging and leading indicators for security performance as they relate to reliable BPS operation. These metrics help inform senior executives in the electricity industry (e.g., NERC's Board of Trustees, management, the Member Representatives Committee, and the Reliability Issues Steering Committee) by providing a global and industry-level view of how security risks are evolving and indicating the extent the electricity industry is successfully managing these risks.

The 2017 report metrics demonstrate that the E-ISAC's efforts are showing positive, tangible results. The number of reportable cyber security incidents affecting customers resulting in loss of load remains at zero, and the number of reportable cyber incidents affecting grid operations was also at zero for the last two years. During 2015 and 2016, no physical security events occurred that caused a loss of load.[13]

NERC takes all cyber incidents seriously. Although significant risks to the grid still exist, the low numbers show that the electricity industry has seen exceptional performance in protecting the grid from security incidents to date.

[12] National Cyber Incident Response Plan.

[13] In late 2014, a physical security event occurred that resulted in loss of load; however, this event was not officially reported until January 2015.

- Reportable Cyber Security Incidents: Responsible entities must report cyber security incidents to the E-ISAC as required by NERC Reliability Standard CIP-008-5 Incident Reporting and Response Planning. For 2015 and 2016, the E-ISAC reported zero cyber security incidents. While this number is a positive observation, it does not necessarily suggest that the risk of a cyber security incident is low; the E-ISAC continues to see a rise in the number of cyber security vulnerabilities.[14]
- Reportable Physical Security Events: Responsible Entities must report physical security events to the E-ISAC as required by the NERC EOP-004-3 Event Reporting Reliability Standard.[15] During 2015 and 2016, one physical security event occurred that caused a loss of load. This near-zero result does not necessarily suggest that the risk of a physical security event causing a loss of load is low, as the number of reportable events has not declined over the past two years. Although this metric does not include physical security events affecting equipment at the distribution level (i.e., non-BES equipment), NERC receives information through both mandatory and voluntary reporting that indicates that distribution-level events are more frequent than those affecting BES equipment.
- CRISP Reporting Statistics: In 2016, CRISP identified intrusion methods used by threat actors with a wide variety of technical prowess and continued to identify and monitor activities of threat actors and their escalating risk to the U.S. electricity industry. In 2016, the E-ISAC saw 41 cases predicated on IOCs provided by CRISP participants that resulted in all-site reports. CRISP all-site reports leverage information sharing device data and all-source intelligence to provide actionable information to support security operations across the CRISP community with company-specific information removed.
- GridEx Participation: This metric compares the number of organizations participating in each of the GridEx security and crisis response exercises conducted by NERC every two years. NERC's large-scale exercise provides electricity organizations with the opportunity to respond to simulated cyber and physical security attacks affecting the reliable operation of the North American grid. From GridEx II to GridEx III, the number of active participating organizations increased by 58 percent, and the number of observing organizations increased by 42 percent.

Future Activities

The electricity industry has made substantial progress in understanding cyber threats and the risks they pose, as well as implementing protections and mitigations. The E-ISAC is helping to keep industry ahead of the threat by being more strategically focused and developing more robust metrics to determine success.

E-ISAC Long-Term Strategic Plan

The E-ISAC Long-Term Strategic Plan, which was developed working closely with NERC leadership and the ESCC Member Executive Committee, builds on the ESCC's 2015 recommendations and discusses improvements needed in 2017 to address current threats, a look at the mid-term range of 2018-2022 to address emerging threats, and what the E-ISAC might look like beyond 2023 if the forecasted issues

[14] ERO Reliability Risk Priorities, RISC Recommendations to the NERC Board of Trustees, November 2016, p. 9 Risk Mapping chart depicts Cyber Security Risk as having high potential impact and relative likelihood of BPS-wide occurrence.
[15] NERC EOP-004-3 Event Reporting Reliability Standard.

continue to develop.[16] Some near-term objectives include: hiring additional analysts; enhancing the E-ISAC portal; increasing the in-house data storage and analysis capabilities; growing the CRISP and CAISS programs; and increasing engagement with Canada, Mexico, and other ISACs and information sharing partners.

New Metrics

NERC and the electricity industry have taken actions to address cyber and physical security risks to the reliable operation of the BPS as a result of potential and real threats, vulnerabilities, and events. As NERC continues to do this in 2017, we are developing metrics that provide a global and industry-level view of how security risks are evolving, and the extent to which the electricity industry is successfully managing these risks. NERC is developing new metrics to:

- Redefine reportable incidents to be more granular, and include zero consequence incidents that might be precursors to something more serious.
- Use CRISP data to run malware signature comparisons to see how many hits occur on a benchmark set of entities and if any of these hits have serious implications for the grid. This metric could be used to provide a percent change from a benchmark year-over-year.
- Use data obtained from CAISS and similar capabilities to characterize the type and frequency of various cyber threats reported through the year.
- Include other data sources such as the FBI, SANS Institute, Verizon, etc., as input for understanding the broader security landscape surrounding critical infrastructures.

Conclusion

NERC's E-ISAC is the electricity industry's central hub for security information sharing and analysis. Working with industry, government, and all stakeholders, the E-ISAC has made substantial progress in anticipating, identifying, and mitigating grid security threats. Data collected by NERC support a trend line showing continuous improvement in a strong culture of security and information exchange. Yet given the evolving nature of threats, there is no end point at which grid security can be forever assured. Security can only be achieved through constant vigilance, agility, and information sharing partnerships. Consistent with these necessities, the E-ISAC's strategic plan provides for continuous evolution with new tools, new capabilities, and enhanced member engagement. I thank the Commission for asking these important questions today and I look forward to the discussion.

[16] *"E-ISAC Long-Term Strategic Plan" at www.eisac.com.*