FERC 2018 Reliability Technical Conference

Panel IV: Addressing the Evolving Cyber Security Threat
Remarks of Bill Lawrence, Director, Electricity Information Sharing and Analysis Center (E-ISAC)
North American Electric Reliability Corporation
July 31, 2018

Introduction

Good afternoon. My name is Bill Lawrence and I am the Director of the Electricity Information Sharing and Analysis Center (E-ISAC) at the North American Electric Reliability Corporation (NERC). Thank you for the opportunity to appear before the Commission to discuss the evolving cyber security threat and the work NERC and the E-ISAC are doing to mitigate potential impacts on the bulk power system (BPS).

Addressing the evolving cyber security threat and 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 at an increasing pace due to geopolitical tensions, changing societal trends, and continuous technological advancement. In addition, the adversary is becoming more sophisticated, and we are seeing more publicly reported and attributed state-sponsored activity across many industries and around the world. NERC and the E-ISAC 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 activities led by our long-term strategic plan, which the NERC Board of Trustees accepted in May 2017. This strategy focuses on three main areas: information sharing, analysis, and engagement. I am pleased to report on our progress to date and our continued strategic focus on the future.

NERC addresses cyber security threats through a variety of regulatory and non-regulatory means. NERC's mandatory Critical Infrastructure Protection Standards (CIP Standards) provide foundational baseline protections to entities subject to the Standards. The CIP Standards have changed considerably with NERC's evolution to a risk-based organization, informed by industry experience and a broadening understanding of threats and vulnerabilities. The Commission has most recently proposed further changes to expand the scope of mandatory reporting of Cyber Security Incidents.[1] Consistent with its comments to the Commission and its recommendation in the 2017 State of Reliability Report, NERC supports broadened reporting of Cyber Security Incidents to allow it to obtain and share additional information to improve the security and reliability of the Bulk Electric System (BES). Pursuant to Commission directive, NERC has also proposed a new CIP Standard addressing supply chain risk management. Once approved and enforceable, this Reliability Standard will require a number of measures to mitigate risk arising from the supply chain. NERC is also working with industry subject matter experts on developing modifications to the CIP Standards to address emerging technologies, such as the use of virtualization. The purpose of these changes is to help ensure the CIP Standards are objective-based and adaptable to future technological innovation.

[1] See Docket Nos. RM18-2-000 and AD17-9-000.

But security cannot be achieved through standards alone, even as the CIP Standards continue to mature by displacing prescriptive requirements more closely coupled to specific practices and technologies with more outcome- and capability-based requirements. Industry also requires the agility to respond to new and rapidly changing events far faster than any standards process could support. 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 shared understanding of "ground truth" during rapidly evolving security events inside and outside the electricity industry. Taken together, mandatory standards coupled with effective mechanisms to share information provide a robust and effective capability to help industry 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.

Overview of the *E-ISAC Long-Term Strategic Plan*

The E-ISAC's mission is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. 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. In 2017, the NERC Board accepted the *E-ISAC Long-Term Strategic Plan*, which the E-ISAC developed working closely with NERC leadership and the ESCC's Member Executive Committee.

The strategy covers three main areas: information sharing, analysis, and engagement. Addressing specific activities under each area helps the E-ISAC understand the threats and manage risk, but more importantly, we are able to better assist our members in protecting themselves against evolving cyber threats.

Information Sharing

The E-ISAC engages in a range of information sharing activities that help identify and 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 and to provide training activities. Also, our biennial Grid Security Exercise (GridEx) is 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.

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 E-ISAC adds value for its members and assists with overall risk reduction across industry.

E-ISAC Portal: Most of the E-ISAC's communications with electricity industry members are via a secure portal that was revamped in 2017, and is currently undergoing upgrades to enhance the user experience. The new portal functions improve bi-directional information sharing and allow members greater access to

more information. This year, the E-ISAC is launching a new user community function in which members can form specific user groups and communicate with each other through those groups.

E-ISAC Critical Broadcast Program: The E-ISAC launched a rapid information sharing capability in 2018—the Critical Broadcast Program (CBP). The CBP capability rapidly disseminates critical security information to electricity industry AOOs. 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. The information is disseminated through the E-ISAC portal and other means, as necessary. The E-ISAC used this capability twice: on February 7, where 1,208 individuals from 245 organizations joined the call; and February 22, where over 960 individuals from 220 organizations joined the call.

Analysis

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 and context team provides analysis on shared information to produce actionable indicators disseminated to members, thereby building on the cyber "big picture." This includes vetting information shared by government and cross-sector partners for validity while also explaining how certain indicators would apply to industry. 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. One main cyber program is the Cybersecurity Risk Information Sharing Program (CRISP).

CRISP is a public-private partnership (cofounded by DOE and NERC, 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 [PNNL]). The purpose of CRISP is to collaborate with industry partners to facilitate the timely bidirectional sharing of unclassified and classified threat information, thereby enabling AOOs 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 industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

The E-ISAC is developing new analytic capabilities to enhance CRISP in collaboration with DOE, PNNL, and strategic vendor partnerships. Enhancements include analyzing SysLogs and email header information, threat detection analysis in the Operational Technology environment, and additional analytic tools and capabilities to improve information technology threat detection.

Engagement

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 leads activities and participates in several forums to help us better understand security risks and provide members with security information and mitigation strategies.

GridEx: NERC conducted its fourth biennial grid security and emergency response exercise, GridEx IV, on November 15-16, 2017. GridEx IV 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 IV was the largest geographically distributed grid security exercise ever conducted. GridEx IV consisted of a two-day distributed play exercise and a separate executive tabletop on the second day. More than 6,500 individuals and 450 organizations across North America participated in GridEx IV, which included representatives from industry, law enforcement, and government agencies.

In March 2017, 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 IV. The reports summarize the exercise and provide recommendations that the E-ISAC has integrated into its internal crisis action plan and standard operating procedures. In addition, the ESCC has adopted many of the recommendations into its playbook and used the GridEx IV 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 to improve security, resilience, and reliability.

GridEx V is scheduled for November 13-14, 2019, and will include an executive tabletop session on the second day.

GridSecCon: The E-ISAC convenes GridSecCon each fall. In 2017, this assembly brought together over 500 electricity cyber and physical security professionals. GridSecCon 2017 provided free training and educational sessions on various technologies, and physical and cyber security issues, such as Mission Dependency Analysis; Threat Modeling, Intelligence Consumption, and Hunting in ICS; and Red Teaming the Micro Grid. The conference included speaker sessions discussing industry's work with government partners, insider threats, geomagnetic disturbances and high-altitude electromagnetic pulse research, and supply chain management. GridSecCon 2018 will take place in Las Vegas, NV, from October 16-19.

Industry Augmentation Program (IAP): The IAP is a three-day immersion program for member company personnel to work inside the E-ISAC to gain deeper understanding of the E-ISAC and its operations. The IAP offers participants an enriched learning experience and an opportunity to build strong, trusted relationships, grow professional networks, and develop a deeper shared understanding of security methodologies, analytical processes, and issues impacting industry. So far, the E-ISAC has partnered with 17 analysts from 13 utilities; the final IAP session in 2018 will be in November, when we host 5 more analysts.

E-ISAC Monthly Briefing Series Update: The E-ISAC continues to host its monthly briefing series for AOOs, covering timely security and CIP topics for participants. The briefings include federal and commercial technical partners, including DHS staff from the Industrial Control Systems Cyber Emergency Response Team, the Office of Intelligence and Analysis, the National Cybersecurity and Communications Integration Center (NCCIC), and threat intelligence companies such as Dragos. Participation in the monthly briefings during 2017 ranged from 180 to over 400 attendees. 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: The E-ISAC hosts 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 holds one workshop in December in Washington, DC; the other workshop location varies each June.

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. The E-ISAC regularly coordinates 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, it allowed the E-ISAC to provide additional insight and analysis on key topics, such as the Ukraine events.

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 2017, the E-ISAC saw 226 cyber bulletins posted to the E-ISAC portal. Of the 226 cyber bulletins, 191 were based on information provided by members or posted by members themselves. This trend is consistent with the 241 cyber bulletins in 2016. The E-ISAC expects this number to increase in 2018 as member participation increases. The E-ISAC also posted several bulletins based on information obtained from government partners and trusted open source partners.

Over 30 percent of the total number of cyber reports involved phishing incidents. Other important trends and analysis that the E-ISAC conducted this year focused on reconnaissance, exploitation, and compromise activities. The E-ISAC observed some activity that leveraged ransomware and other activities that used compromised credentials and technology native to the target environment. The E-ISAC also monitored several non-industry specific campaigns, including WannaCry and NotPetya ransomware activity.

Malware Targeting Safety Instrumented Systems (SIS): In November 2017, Dragos Inc. and FireEye identified new malware that targeted SIS devices. Dragos directly shared analysis and threat information on this malware with the E-ISAC. The malware can disable the SIS protection, leaving critical industrial control systems vulnerable to failure without the safety trip from the SIS. The E-ISAC provided members with specific recommendations for protecting against this malware. The E-ISAC has not received any reports of malware targeting SIS systems being found on systems within NERC's footprint.

Malware Targeting Electricity Industry Assets in Ukraine: In June 2017, the E-ISAC released information on modular malware samples that may have been involved in the December 2016 attack on Ukraine's electricity assets. The reports include details of the malware's capabilities. The information was shared with the E-ISAC by industrial control security company Dragos Inc. NERC amplified this information in a Level 1 (Advisory) NERC Alert on June 13, 2017, entitled "Modular Malware Targeting Electricity Industry Assets in Ukraine." The malware is a modular framework that can be tailored to meet desired objectives against specific equipment in the target environment. The malware sample analyzed included capabilities against ABB and possibly Siemens equipment. The malware's framework design likely allows for the targeting of other vendors or communication protocols.

In July 2017, the E-ISAC and SANS Industrial Control System (ICS) Team released a joint product summarizing analysis of the modular malware framework associated with the 2016 attack on Ukraine's power system. The report consolidated open source information, clarified important details surrounding the attack, offered lessons learned, and recommended approaches to help the ICS community search for and repel similar attacks.

The TLP:AMBER version of the Defense Use Case contains considerations specifically for electricity industry AOOs. A TLP:WHITE version was also released without the industry-specific considerations. The E-ISAC recommended that members evaluate their ICS environments for abnormal activity that matches the malware. The E-ISAC is not aware of any North American electricity companies being targeted or compromised by this malware.

Advanced Persistent Threat Actor Targeting the Electricity Industry and Other Critical Sectors: In June 2017, the E-ISAC released a Level 1 (Advisory) NERC Alert to inform NERC registered entities of a campaign targeting several critical sectors, including the electricity industry. The FBI and DHS released the *Joint Analysis Report* (*JAR*), *JAR-17-20114*, on advanced persistent threat (APT) actors targeting energy, nuclear, and critical manufacturing industry companies, including electricity industry members in the United States.

APT actors have attempted to collect and compromise energy industry credentials. The credential harvesting campaign used website water-holing and spear phishing to trigger external authentication attempts via Server Message Block (SMB). The remote authentication attempts caused credentials to be exposed outside the protected network, and they were likely compromised. According to the JAR, the compromised credentials may have been used to access the victim's environment. Once inside the environment, the APT actors used native network management and monitoring tools to collect additional information, including additional authentication information and possibly establish persistence.

In July 2017, the FBI and DHS released an update to *JAR-17-20114* that expanded the list of targeted entities to include government organizations as well as water and aviation sectors members. The update also provided additional indicators of compromise and more details into the tactics, techniques, and procedures (TTP) the threat actors used.

In September 2017, Symantec published a report tying this activity to an APT group called "Dragonfly" (i.e., Energetic Bear, Koala, and Iron Liberty). In October 2017, the E-ISAC's monthly webinar featured Vikram Thakur, Technical Director at Symantec, who discussed Symantec's findings and provided additional information for electricity industry members. The E-ISAC, Symantec, and other security researchers agree that the activity reported indicates high interest in electricity industry companies and that the actors have a high level of sophistication. The E-ISAC recommended that members remain highly vigilant of this threat and informed on campaigns that continue to target electricity companies. The E-ISAC posted additional information regarding Dragonfly on the E-ISAC portal.

Targeting the Electricity Industry: In mid-November 2017, the FBI released a TLP:AMBER report detailing indicators of cyber activity from August through September targeting the electricity industry. The information in the FBI report appears to match other industry targeted activity shared through the E-ISAC from mid-2017 to December 2017. Sophisticated and coordinated actors appear to have increased interest in compromising electricity industry members.

Supply Chain Security Risks: To implement a stronger supply chain risk management security posture for the U.S. Government, on September 13, 2017, DHS issued *Binding Operational Directive* (*BOD*) *17-01,* which notified all executive branch agencies "to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities." This document describes the directive and the reasoning behind it, and offers recommendations and additional information on supply chain risks to the North American BPS.

The E-ISAC released a Level 2 (Recommendation) NERC Alert on October 5, 2017, to inform NERC registered entities of supply chain risks in relation to a directive to executive branch agencies by DHS and to request information to assess the extent of exposure of the BPS Analysis of the responses showed that 98% of registered entities either had no Kaspersky-branded products known to be in use within BES Cyber Systems, or had plans to mitigate the risks of known use.

Large IoT Botnets: In September, 2017, CheckPoint and Netlab360 reported that more than one million devices may be part of a botnet larger than the Mirai botnet which appeared in 2016. The new botnet has been named "IoTroop" or "IoT_reaper." The E-ISAC previously reported on risks associated with Internet of Things devices, including the 2016 release of a Level 2 (Recommendation) NERC Alert to registered entities.

Phishing: Spear phishing and whaling accounted for approximately 15 percent of phishing emails reported. Phishing will likely remain the prevalent delivery method for cyber attacks in 2018. End-user training, email monitoring, and attachment testing technologies may help members combat this threat. Toward the end of 2017, reports pointed to an increase in phishing activity originating from trusted businesses that may have been compromised. Phishing emails may appear simple and benign by design to maximize their relevance to a significant subset of employees at a large organization.

NERC-Themed Phishing: In early November, 2017, several E-ISAC members, NERC staff, and E-ISAC staff received a phishing email that appeared to originate from NERC. The email had a subject of "Your Copy" and a PDF attachment. The attachment contained a hyperlink that redirected to a credential harvesting site. NERC and the E-ISAC responded quickly and prevented any credentials from being compromised. The E-ISAC promptly informed industry members, and we do not believe any credentials were compromised as part of this phishing activity. The E-ISAC recommended that members consider out-of-band credential resets for users who may have shared credentials with untrusted websites.

Credential Harvesting Attempts: Throughout 2017, the E-ISAC received a significant increase in spear phishing reports with credential harvesting objectives, and members observed several instances of SMB protocol credential harvesting. The E-ISAC believes spear phishing and exploitation of SMB misconfigurations may continue to be used as an effective adversary technique to collect and ultimately compromise credentials. The E-ISAC believed that this was coordinated activity targeting the electricity industry and provided several mitigation activities to members.

2018 Cyber Security Outlook

The E-ISAC is looking at the following trends for 2018:

Continued and more sophisticated phishing activity: The E-ISAC has seen an increase in sophisticated phishing activity against our members. Recent phishing activity has focused on the technique of directing victims to a malicious site to harvest their credentials.

Continued exploitation of established trust relationships with business partners: External partners with potentially less effective security postures are attractive initial targets because they may be more likely to open a phishing email from a trusted source.

Cryptocurrency mining: As long as the value of cryptocurrency continues to remain high, the E-ISAC expects illegitimate cryptocurrency mining activity to continue as it becomes a part of the global cyber threat

activity baseline. This activity may not be specifically targeted at the electric industry but nonetheless poses a security risk.

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, grid security cannot 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.