NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Reliability Technical Conference

Panel III: 2016 State of Reliability Report

Remarks of Marcus Sachs, Senior Vice President and Chief Security Officer
North American Electric Reliability Corporation
June 1, 2016

Chairman Bay, Commissioners, staff, and fellow panelists. My name is Marc Sachs and I am a Senior Vice President and the Chief Security Officer at the North American Electric Reliability Corporation (NERC). I greatly appreciate the opportunity to participate in today's reliability technical conference. Grid security is a constant and ever-evolving threat requiring perpetual vigilance. I will focus in particular on the following subjects:

- The Cybersecurity Information Sharing Act of 2015 (CISA 2015), the Fixing America's Surface Transportation (FAST Act), and how provisions in both new laws will help address cybersecurity risks and enhance information sharing;
- Lessons learned from recent cyber attacks, and our response;
- The spare transformer plan under development by the Department of Energy (DOE); and,
- Ongoing electromagnetic pulse research.

Current Grid Security Efforts

As NERC's Chief Security Officer, I am the senior officer of the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC is a leading source for voluntary information sharing for many in the Electricity Subsector. It gathers information from electricity industry participants across North America about security-related events, disturbances, and off-normal occurrences within the Electricity Subsector and shares that information with other electricity industry participants, key governmental entities, and cross-sector partners. Governmental entities and cross-sector partners also provide the E-ISAC with information regarding risks, threats, and warnings that the E-ISAC disseminates throughout the Electricity Subsector. Two-way information sharing is critical because it allows the E-ISAC to help industry identify emerging trends and to provide an early warning, particularly in today's ever-changing security environment.

The threat of cyber and physical attacks on the grid by nation states, terrorist groups, and criminal actors is at an all-time high; the challenge will continue to grow exponentially. NERC is working hard to provide effective leadership, in coordination with our public and private partners, in securing the grid.

Protecting critical infrastructure from cyber and physical threats and vulnerabilities requires diverse defense strategies. NERC's mandatory Critical Infrastructure Protection (CIP) Standards are one piece of a complex, dynamic, and comprehensive approach to grid security and reliability. The public/private partnership NERC has through the Electricity Subsector Coordinating Council (ESCC), which addresses resiliency and reliability issues, has greatly improved the conversation among government, industry, and NERC. The Department of Energy (DOE) is also a key partner with NERC in addressing, identifying, and analyzing security needs of the grid. These efforts are complemented by research and technology

development by DOE's national laboratories. This work has significantly helped promote computer-to-computer monitoring and information exchange. And finally, NERC's E-ISAC is an essential information sharing hub that provides situational awareness, incident management, coordination, and communication capabilities within the Electricity Subsector through timely, reliable, and secure information exchange.

The E-ISAC uses a variety of tools, programs, and activities to enhance security, such as a secure web portal, alerts, exercises, training and education. Among our programs, the annual Grid Security Conference brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, training, and lessons learned. Over the past few years, the E-ISAC's efforts and impact on the electricity industry have grown, resulting in increased budget and staff to build on the products, tools, and services offered to both industry and our government, and cross-sector partners.

The E-ISAC portal, for example, allows the E-ISAC to reach thousands of industry members and hundreds of organizations across the subsector and is the mechanism for industry and government to contact E-ISAC staff with questions, concerns, and security-related information in a secure manner. Over the past year, we have enhanced the portal and continue to make improvements to meet our members' needs. The data we receive from industry members and partners helps the E-ISAC create timely, relevant, and actionable documents. Some of the products the E-ISAC develops include daily, weekly, and monthly reports; incident bulletins; and issue-specific assessments. E-ISAC staff also advises the NERC Bulk Power System Awareness team on the issuance of NERC Alerts regarding cyber and physical security vulnerabilities.

The E-ISAC also coordinates GridEx, a biennial grid exercise that is designed to exercise utilities' crisis response and recovery procedures, improve information sharing during a crisis, gather lessons learned, and engage senior leadership. GridEx III, which we held in November 2015, was a very successful exercise that included over 4,400 registered participants from 364 organizations across North America. In addition, 30 industry and government senior leaders participated in a tabletop exercise. The recommendations from the exercise focused on unity of messaging, unity of effort, and extraordinary measures.

Finally, the Cybersecurity Risk Information Sharing Program (CRISP) is a voluntary NERC program managed by the E-ISAC that facilitates the exchange of detailed cybersecurity information among industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory. The program enables owners and operators to better protect their networks from sophisticated cyber threats. The purpose of CRISP is to facilitate the timely sharing of government enhanced threat information, enhance situational awareness, and better protect critical infrastructure.

Outside of the E-ISAC, NERC participates in the ESCC – a key organization representing all segments of the electricity industry. It is the only sector coordinating council exclusively comprised of chief executive officers and is an outstanding example of a strong public-private sector partnership. The ESCC provides key communication with our government partners, coordinating efforts related to disasters and threats to critical infrastructure. Its government counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

Together, the ESCC and the E-ISAC enhance the subsector's security efforts. The ESCC has called for the E-ISAC to be the central source of information sharing between the Electricity Subsector and the government. This support for the E-ISAC's role in information sharing has led to increased awareness and improved communication on its operation and performance initiatives.

Cybersecurity Information Sharing Act of 2015 & Fixing America's Surface Transportation Act

In December 2015, the President signed into law both CISA 2015 and the FAST Act, two laws that include cybersecurity provisions impacting the E-ISAC and our relationship with our government partners. Specifically, CISA provides for voluntary information sharing between the private sector and government, authorizing sharing procedures. The Department of Homeland Security's National Cybersecurity and Communications Integration Center is designated as the Federal civilian interface for multi-directional and cross-sector information sharing related to cybersecurity risks, incidents, analysis, and warnings.

In seeking to enhance voluntary information sharing, CISA recognizes that existing, effective sharing relationships should be preserved and strengthened. Accordingly, CISA includes several provisions that should further strengthen relationships with NERC, the E-ISAC, industry, and the government — and ultimately enhance information sharing. These provisions include:

- A requirement that information sharing procedures incorporate existing sharing relationships, including ISACs.
- Preservation of contractual obligations related to information sharing relationships.
- Clarification that nothing in CISA shall conflict with mandatory standards.

With respect to the FAST Act, Congress granted DOE new authority to issue emergency orders following a presidential declaration of a grid security emergency. Before issuing an order, DOE is required to consult to the extent practicable with numerous entities, including, among others, the Commission, the Electric Reliability Organization (ERO), industry, and appropriate authorities in Canada and Mexico. This authority addresses a gap that previously existed and will help build upon existing relationships and partnerships with DOE.

The FAST Act also provides the Commission with new authority with respect to the secure handling and protection of Critical Electric Infrastructure Information (CEII) shared by industry. This provision exempts CEII from disclosure under the Freedom of Information Act for a five year period, subject to extension by the Commission. Industry is more likely to share sensitive information when protection of shared information is assured. We believe this additional protection can enhance voluntary information sharing.

Finally, the FAST Act includes a provision requiring DOE to develop a strategic transformer reserve plan for submittal to Congress. The plan will evaluate the feasibility of a strategic transformer reserve program, including emergency mobile substations. DOE is required to consult with numerous entities, including the Commission and the ERO. NERC is currently providing DOE with technical assistance and subject matter expertise to help develop the plan. DOE is making progress, and NERC is pleased to be part of this important effort.

Recent Attacks – Lessons Learned

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015, have garnered significant attention. The illegal intrusions by a third party into the company's computer and Supervisory Control and Data Acquisition systems affected up to 225,000 customers in three distribution-level service territories and lasted for several hours. The events in Ukraine are a reminder that cyber threats are real and that constant vigilance is needed to protect the reliability of the North American grid. At the same time, it is important to note that the operational and technical aspects of the North American bulk power system (BPS) are different from those of the Ukrainian system. Other differences include the U.S. industry's mandatory and enforceable cyber security standards, including security management controls and authorized personnel and training controls; network segmentation; and the use of licensed anti-virus software, among other things.

Following the attacks, the E-ISAC and the SANS Internet Storm Center (SANS ISC) developed a joint report that is publicly available on the NERC website.[1] The report includes an industrial control system cyber kill chain mapping, which helps companies understand how an attacker formulates a plan. The report provides defense lessons and basic cybersecurity tools and practices companies can use to prevent or disrupt a cyber attack. It also offers potential techniques for preventing or disrupting future attacks. Specific issues mentioned in the report include spear phishing, credential theft, data exfiltration, VPN access, and workstation remote access, among other topics.

On February 9, 2016, the E-ISAC issued a Level 2 Alert based upon findings from the cyber attacks in Ukraine. The NERC alert is one tool for providing concise, actionable information to the electricity industry. As a Level 2 Alert, it recommends registered entities take specific actions, and requires a response by recipients.

Of utmost importance, we learned from this experience that the North American Electricity Subsector is moving in the right direction with appropriate protections, including mandatory CIP Standards, advanced technologies, partnerships with industry and government, and information sharing about threats and vulnerabilities.

Electromagnetic Pulse (EMP) Research

NERC and industry recognize the potentially serious risks posed by High-Impact, Low Frequency (HILF) events. Over the past several years, the industry's preparedness for the unique challenges of HILF events has advanced through coordinated actions involving industry experts, public and private researchers, commercial developers, and policy stakeholders. The approach is effective in addressing technically-complex HILF risks, like Geomagnetic Disturbances and EMP, because it engages individuals with specialized expertise, threat knowledge, and power system experience in collaborative efforts.

Recently industry, led by the ESCC, has enhanced efforts to address EMP risks to the electric grid through the establishment of an EMP Task Force and support of an Electric Power Research Institute (EPRI) research

[1] *Analysis of the Cyber Attack on the Ukrainian Power Grid*, NERC, March 2016.

project. The research project will work in partnership with the Department of Defense, DOE, the National Labs, and electric power companies to better understand impacts and vulnerabilities in the electric grid, analyze mitigation and recovery strategies, and evaluate measures for increasing system resilience. NERC supports these efforts led by the ESCC and is committed to sharing information and best-practices throughout the industry.

Conclusion

To keep up with the changing threat landscape and enhance grid security across North America, we have to be dynamic and nimble. The E-ISAC understands this and continues to increase and improve its products and services to members and partners. We continue to encourage and facilitate greater information sharing, improve tools, engage in exercises, and share lessons learned. We are encouraged by newly-enacted authorities to facilitate information sharing and strengthen security of the BPS. I appreciate the opportunity to discuss critical security challenges with the Commission and I look forward to your questions.