Testimony of Manny Cancel
Chief Executive Officer, Electricity Information Sharing and Analysis Center,
and Senior Vice President, North American Electric Reliability Corporation

Before the Subcommittee on Oversight and Investigations,
U.S. House Committee on Energy and Commerce

"Examining Emerging Threats to Electric Energy Infrastructure"

July 18, 2023

Thank you Chairman Griffith, Ranking Member Castor, and members of the committee. I am pleased to testify today concerning threats to the security of the nation's electric grid. As chief executive officer of the Electricity Information Sharing and Analysis Center (E-ISAC), I appreciate the subcommittee's interest in examining the highly complex and continuously evolving threat environment, and actions to address security risks. Reliable delivery of electricity is essential to every aspect of life in the United States. While there has been no loss of load to date in North America that can be attributed to a cyber attack, grid security requires continuous vigilance and agility. The E-ISAC plays an important role in helping protect the grid from malicious cyber and physical threats. This testimony will summarize these E-ISAC activities and the current threat landscape.

About the E-ISAC – Key Programs and Partnerships

Operated by the North American Electric Reliability Corporation[1] (NERC) and created in 1999, the E-ISAC serves as the clearinghouse for security information for the electricity industry in North

[1] NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system (BPS) through system

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

The E-ISAC operates a 24/7 watch operation, develops expert in-house analysis of ongoing incidents, and provides a suite of analytical products and services accessible through the secure E-ISAC Portal to over 1,700 member and partner organizations. The E-ISAC plays a key role in cross-sector coordination, engaging with sectors and their ISACs that have a critical interdependence with electricity, including oil, natural gas, and water, and other critical infrastructure sectors, such as finance and communications. We work in collaboration with these cross-sector partners to break down information sharing silos between industry and government to promote broad awareness of threats and mitigations.

We collaborate closely with the Department of Energy (DOE), the Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the National Counterterrorism Center (NCTC), and the Electricity Subsector Coordinating Council[2] (ESCC) to further partnerships

awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight in the United States by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves nearly 400 million people.

[2] The CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry on efforts to prepare for, and respond to, national-level disasters or

that are vital to addressing security. It should also be noted that NERC and the E-ISAC are members of the ESCC and that the E-ISAC works in close collaboration with the ESCC secretariat to operationalize ESCC initiatives. In addition, the E-ISAC maintains similar relationships with partners in Canada.

The E-ISAC is organizationally isolated from NERC's enforcement processes to facilitate and maintain a culture of voluntary information sharing and trust. NERC and the E-ISAC adhere to a strict Code of Conduct. It is important to note that NERC's regulatory programs complement the E-ISAC's activities to strengthen grid security. North America's high voltage electric transmission system is subject to a suite of mandatory cyber and physical security standards, known as the Critical Infrastructure Protection (CIP) standards, enforced by NERC and FERC. The CIP standards provide a common, universal foundation for security. They are robust and comprehensive, covering a wide range of priorities and threat vectors. The CIP standards provide a common set of essential practices. Given the dynamic nature of the threat environment, standards must be complemented with the analysis and sharing of threat and vulnerability information to enhance situational awareness and share mitigation tactics. The E-ISAC provides the type of timely, actionable information needed to complement the regulatory framework and strengthen the security posture of the electricity sector. General insights and trends observed by the E-ISAC can also inform improvements to mandatory standards, as warranted.

threats to critical infrastructure. The ESCC works across the sector, and with the E-ISAC, to develop actions and strategies that help protect the North American energy grid and prevent a spectrum of threats from disrupting electricity service.

Key E-ISAC activities, programs, and partnerships include:

Secure Portal – Information is exchanged through the E-ISAC's secure portal through posts by members and partners, and the E-ISAC. Members and partners use the portal to voluntarily share information with the E-ISAC, which analyzes shared information for the benefit of the community. The E-ISAC also uses the portal to communicate threat warnings and mitigations, and provide analytical products that provide actionable context to support industry security personnel. Many products posted to the portal are a collaborative effort between E-ISAC analysts and industry.

Bulletins and Alerts -- In addition to the secure portal, NERC Alerts are an industry-recognized program to provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Depending on the Alert level, NERC can require industry participants to respond concerning their progress in implementing mitigation measures. Recent security-related Alerts have covered such topics as supply chain risks, like the SolarWinds incident, preparation for potential Russian cyber activities, communication of a prohibition order securing critical defense facilities, and the Log4j vulnerability. For rapid, elevated, industry-wide awareness requiring immediate action, the E-ISAC also issues All-Points Bulletins and conducts Critical Broadcast Program calls, often within hours of a major event or incident. Examples include the recent U.S. Government and Microsoft report on Volt Typhoon. This suite of bulletins and alerts ensures industry is aware of the most significant threats and the mitigations necessary to defend the grid.

Cyber Threat Analysis Programs – The E-ISAC provides a suite of capabilities tailored to the industry's cyber analysis needs to address the threat landscape. The Cybersecurity Risk Information Sharing Program (CRISP) is a premier example of the E-ISAC's partnership with DOE. Managed by the E-ISAC, CRISP uses unique technology, leveraging DOE and its National Laboratory System's analytical capability to provide cyber threat intelligence and government-informed reporting to help North American asset owners and operators detect threats that utilities cannot get anywhere else. CRISP participants cover more than 90 percent of U.S. customers, who receive timely bi-directional sharing of unclassified and classified threat information. Utilities use this critical situational awareness tool to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP information is further shared in a secure fashion through the E-ISAC portal, and allows non-CRISP companies to benefit from the shared indicators and threat actor activity captured by the program. In the nine years since its inception, CRISP has continued to grow its capabilities, and we are working closely with the participating utilities, the labs, and DOE to grow and evolve the program to face expanding threats from nation-states like China and Russia. E-ISAC analysts, in-turn, conduct proactive threat hunting in CRISP data and other data sets like Neighborhood Keeper, Essence, and other tools to identify additional threats based on the tools and information available. These threat hunts have helped identify additional gaps and enabled industry to apply additional mitigations. This analysis is complimented by partnerships with cross-sector ISACs like the Downstream Natural Gas, Oil and Gas, Telecommunications, Financial Services, Water, and others. The E-ISAC also collaborates with cyber security firms like Dragos and Mandiant to

provide additional information and analytical capabilities to ensure industry has access to best-in-class IT and OT information.

Energy Threat Analysis Center (ETAC) and Government Engagement – The E-ISAC is part of the newly established Energy Threat Analysis Center (ETAC), a DOE-led initiative that features collaboration between electric industry partners and government agencies through DHS Cybersecurity & Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative. The ETAC will serve as a spoke to the Joint Cyber Defense Collaborative hub, and enable operational intelligence collaboration for the entire energy sector, and the E-ISAC is proud to be part of the pilot to stand up this capability. ETAC partners meet regularly in classified and unclassified environments to discuss threats and to provide industry context to the intelligence community, and collaborated on threats emanating from the Russian war in Ukraine, supply chain events, and operational technology vulnerabilities. This is an important example of how the private sector is working with government to defend critical infrastructure.

Trainings, Briefings, and Workshops – To help understand the evolving threat environment and mitigations, the E-ISAC provides members and partners with regular trainings, briefings, and workshops. In response to the emerging and diverse physical security threats to the bulk power system (BPS), the E-ISAC has conducted specific and actionable workshops to provide utilities with mitigation strategies that lead to upgrades at their facilities, thereby enhancing protective measures in defense of physical security attacks. Following the December 2022 substation attacks in Moore County, North Carolina, the E-ISAC held a special webinar and briefing with over

1,000 participants to detail the incident, response, and mitigation strategies. Similar briefings have also been held around cyber events.

E-ISAC workshops teach the design basis threat methodology (DBT). The DBT is a scenario-based methodology that focuses on detection, assessment, and response. It helps utilities identify unacceptable consequences and leads to determining specific upgrades to ensure those consequences do not occur. The E-ISAC has conducted 18 of these workshops since 2017 across a diverse subset of our membership. The E-ISAC will host three more workshops in 2023, and we already have four in place in 2024. CRISP, GridEx, and GridSecCon also provide opportunities for hands-on cyber security training, using realistic scenarios based off real world events.

GridEx – The largest grid security exercise in North America, GridEx is hosted every two years by the E-ISAC. The exercise gives E-ISAC member and partner organizations a forum in which to practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. The seventh GridEx will be held this November.

GridSecCon – This annual conference convenes hundreds of grid security experts from industry and government to participate in trainings, collaboration, policy discussion, and sharing of best practices. Specific learning opportunities include topics such as ballistic damage, Vulnerability of Integrated Security Analysis workshops, domestic violent extremist panels, roundtable discussions on security challenges, incident tracking, and sabotage criteria.

Industry and Vendor Engagement – Recognizing the increased interdependencies and complexities in the supply chain among security, vendors, and the electricity industry, the E-ISAC Vendor Affiliate Program facilitates information sharing and best practices. In the year since its inception, the Vendor Affiliate Program now has ten members representing manufacturers and security firms widely used by the electricity community. We expect continued growth within this community and will leverage it to help mitigate the supply chain threat.

The Threat Landscape

The threat landscape includes continuously evolving and persistent threats from sophisticated, capable, and diverse adversaries. Among the most pernicious are nation states, which possess the capability to disrupt critical infrastructure in North America. Numerous reports issued by the U.S. and Canadian governments, including the U.S. Intelligence Community's Annual Threat Assessment, underscores the severity of the threat faced by critical infrastructure from nation-state and transnational criminal actors. Aided by a significant increase in software and hardware vulnerabilities, adversaries are constantly looking for ways to exploit electricity sector participants.

Chinese cyber activities are probably one of the largest and most dynamic cyber threats to critical infrastructure and continue to demonstrate an increasing sophistication, including new and adaptive techniques to gain access to networks, and conduct espionage. Russia remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and its allies. North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat.

Ransomware attacks are common and growing in frequency and sophistication. The FBI's *2022 Internet Crime Report* states that they received 870 critical infrastructure ransomware complaints that year, including 15 from the energy sector.[3] Of the 16 critical infrastructure sectors, 14 had at least one ransomware victim. Recent ransomware attacks perpetrated by groups like Cl0p, Black Basta, and Royal remain a significant concern for the industry, and we continue to work with members, CISA, and law enforcement to share the latest mitigations to assist industry. The MOVEit file transfer breach and extortion scheme perpetrated by Cl0p in particular underscores the significant challenge of ransomware and its impact on supply chain security, with hundreds of widely used vendors being listed as victims.

In May 2021, a ransomware attack to the IT network of the company operating the Colonial Pipeline caused a shutdown of the pipeline for several days. The shutdown disrupted petroleum shipments throughout the East, causing gasoline shortage in many areas. The Colonial attack was a wakeup call over both pipeline security protections and critical sector interdependencies. Had the same event occurred to a natural gas pipeline serving key electricity generators during a severe cold weather event, the human consequences could have been even more significant.

Given the complexity and diversity of systems and equipment that operate the grid, supply chain risk is a significant concern. According to the National Institute for Standards and Technology (NIST), there have already been 15,000 new vulnerabilities in 2023, on track to overcome the

[3] *See report:* 2022_IC3Report.pdf

previous record of over 25,000 set last year.[4] With the number of software and hardware vulnerabilities ever increasing, there is a risk of compromise through a utility's supply chain or trusted vendor. As mentioned above, the E-ISAC is tracking the growing list of MOVEit related victims,[5] and highlighting those firms or manufacturers with significant penetration in the electricity sector.

Physical attacks on electricity infrastructure are deeply concerning. There were almost 1,700 physical security incidents reported to the E-ISAC in 2022, an increase of 10.5% from 2021. Typical physical security incidents against the grid involve vandalism, tampering, arson, and ballistic damage.

Most of these do not result in grid impacts. But a trend toward more serious events occurred in 2022. In November 2022, a series of attacks occurred at six different substations in Oregon and Washington State, five of which resulted in power disruptions. Shortly thereafter in December, a ballistic attack against two substations in Moore County, North Carolina, targeted the substations' transformer radiators and their circuit breakers. This resulted in the substations removal from service, forcing five additional undamaged substations to be powered down and resulted in outages for approximately 42,000 customers during a December cold spell. Last December, damage to two substations in the Seattle-Tacoma area resulted in outages during the Christmas holiday. While arrests were made in the case of these attacks, all too often perpetrators are not apprehended, underscoring the difficulty in ascertaining motive and intent.

[4] NIST, National Vulnerability Database, https://nvd.nist.gov/general/nvd-dashboard
[5] E-ISAC Count is 155 as of July 13, 2023

These recent high profile events are deeply concerning for their sophistication and effectiveness, even while noting that customer impacts were localized. And in February 2023, law enforcement effectively thwarted a plot by domestic extremists to attack five substations in the Baltimore area with an eye toward disrupting service to the majority of the city.

Following the Moore County events, the ESCC convened to share insights and coordinate industry response. In January, ESCC leadership decided to have the E-ISAC and industry trade associations collaborate to develop and share a physical security resource guide that detailed broader considerations in developing a physical security approach for all assets beyond those identified as critical by NERC's physical security Reliability Standard, CIP-014-3.

Recognizing the increase in physical attacks and a need to evaluate adequacy of the physical security standard in the evolving risk environment, FERC ordered NERC to conduct a study evaluating CIP-014-3. Several initiatives came out of this study, including clarification to how entities conduct risk assessments of their substations and a technical conference scheduled for August 10 to consider additional actions. In close partnership with the ESCC, and in response to the increased physical security threats to industry, as well as the uptick in targeted physical security incidents events, the E-ISAC, industry trade associations, regional entities, DOE, PNNL, and FERC are hosting regional events focused on physical security. These events are intended to allow the electric sector industry, government partners, local and federal law enforcement entities, and our regional partners to have a thoughtful and actionable discussion on the current threat landscape, provide mitigation strategies, protective measures, and resources, and strengthen information sharing relationships. The hope is this event and subsequent discussions will demonstrate the continued focus on physical security within the electric sector to key

stakeholders, reinforce relationships with local, state, and federal law enforcement and government partners, and socialize physical security resources available to industry. The E-ISAC is coordinating participation with the NCTC, the FBI, local utilities, DOE, SERC Reliability Corporation, and others, as well as providing the main threat briefing and detailing the response, while providing mitigation strategies to industry with valuable context.

Among other related risks, domestic violent extremists continue to be at the forefront of the threat against critical infrastructure. Insider threat risk presents an incredibly difficult threat to detect and assess. As the technology continues to evolve, unmanned aerial surveillance vehicles (drones) are another concern.

Recommendations

As the subcommittee continues its examination of threats to grid security, Congress should consider the following actions:

National Cybersecurity Strategy – Released in March 2023, the *National Cybersecurity Strategy* recognizes that the complex threat environment and evolving technologies demand a more intentional, coordinated, and well-resourced approach to cyber defense. The five key elements include (1) defending critical Infrastructure, (2) disrupting and dismantling threat actors, (3) shaping market forces to drive security and resilience, (4) investing in a resilient future, and (5) forge international partnerships to pursue shared goals. Congress can facilitate implementation of these strategies in areas requiring legislative action, including support for the authorization and funding of the ETAC.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 – Signed in March 2022, DHS is currently in the process of implementing this new law, which will require critical infrastructure entities to report cyber incidents and ransomware payments to DHS. As implementing regulations are developed, to the extent practicable, the reporting requirements should harmonize with existing requirements currently applicable to the electricity sector under NERC's Reliability Standards. NERC has provided official comments on these points to DHS. Utilities face a variety of federal and state cyber reporting regulations, often with different requirements. Streamlining the required information and process will increase reporting and information sharing.

Conclusion

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. Recent physical attacks show that these types of attacks can disrupt electric service, even as the impact of those experienced thus far were localized. NERC and the E-ISAC address cyber threats through a comprehensive range of complementary strategies. Partnerships with DOE and other agencies are critical. 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 collaboration with industry is key to successful information sharing within the electricity sector and across sectors. Whatever can be done to harmonize reporting requirements and encourage information sharing, especially

automated sharing, will help utilities and government better protect critical infrastructure. NERC and the E-ISAC remain keenly focused on our mission to assure reliability of the BPS.

The electricity industry has taken a defense-in-depth approach for decades. Its culture of mutual assistance and aid emphasizes sharing resources and expertise to ensure the lights stay on or get back on as safely and quickly as possible. Cyber and physical security are no different. The ESCC, in partnership with DOE, CISA, and the White House, continue to emphasize collective defense, and have developed concepts like cyber mutual assistance, response playbooks, and the development of resilient communications activities to help the industry prepare for and respond to these types of incidents. The subcommittee and the American people can be assured that NERC, the E-ISAC, and the industry are working 24/7 to ensure a secure and reliable grid in the face of significant threats.