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

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

"Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid"
December 2, 2025

SUMMARY OF TESTIMONY

E-ISAC Role and Mission

The E-ISAC, operated by NERC since 1999, serves as the central clearinghouse for security information for the North American electricity industry. Its mission is to reduce cyber and physical security risks by sharing trusted, timely, credible, and actionable information and analysis with over 1,900 member and partner organizations. The E-ISAC operates a 24/7 watch operation and collaborates closely with various U.S. government departments (DOE, DHS, FERC, FBI) and cross-sector partners (oil, natural gas, water).

The E-ISAC's information sharing is voluntary and organizationally isolated from NERC's enforcement programs to maintain trust. NERC also enforces mandatory Critical Infrastructure Protection (CIP) standards, which complement E-ISAC activities by providing a universal foundation for security measures such as access controls, malware prevention, incident response, physical protections, and supply chain risk management.

Key Programs and Partnerships

The E-ISAC utilizes several programs to enhance grid security and situational awareness:

- **E-ISAC Portal, Bulletins, and Alerts:** A secure portal and alert system communicate threat warnings, mitigations, and analytical products, sometimes requiring mandatory industry responses to implementing mitigations.
- **Cybersecurity Risk Information Sharing Program (CRISP):** A premier partnership with DOE that leverages national laboratory analysis to provide unique, government-informed cyber threat intelligence, with participants covering over 90% of U.S. customers.
- **Energy Threat Analysis Center (ETAC):** A new DOE-led initiative where E-ISAC partners meet regularly to collaborate on operational intelligence and industry context for the intelligence community.
- **Training and Exercises:** The E-ISAC hosts workshops on physical security methodologies, the biennial GridEx exercise (largest grid security exercise in North America), and GridSecCon, an annual conference for industry and government experts.
- **Vendor Affiliate Program:** A program bringing original equipment manufacturers and security solution providers into the community to facilitate information sharing regarding supply chain risks.

The Threat Landscape

While no loss of load has been attributed to a cyberattack to date, the threat landscape is dynamic and requires continuous vigilance. Nation states, sophisticated criminal actors, and hacktivists pose persistent and evolving threats.

- **Nation-State Actors:**
  - **China:** Salt Typhoon and Volt Typhoon are some of the largest and most dynamic threats, focusing on persistent access and espionage with the potential for future disruption.
  - **Russia:** Focus remains primarily on Ukraine and NATO affiliates, utilizing hacktivist groups and cyber espionage, but tactics could be adapted for North America.
  - **Iran:** Monitored for potential retaliation against U.S. infrastructure amid tensions, often using DDoS attacks.
  - **North Korea:** Deploys thousands of IT operatives using fabricated personas and AI tools to secure remote jobs in North American companies to gain high-level network access.
- **Other Threats:** The E-ISAC monitors domestic hacktivists mentioning physical attacks and persistent ransomware operations.

Recommendations for Congress

- **Authorize ETAC:** Provide congressional authorization for the DOE-led Energy Threat Analysis Center to establish the partnership and advance its mission.
- **Support Funding for CRISP +30 and ONG Programs:** Ensure sufficient funding for programs that help smaller utilities and oil/natural gas companies access critical intelligence and improve situational awareness.
- **Reauthorize CISA 2015:** Reauthorize the Cybersecurity Information Sharing Act of 2015 to support the broader information sharing ecosystem between the private sector and government.

INTRODUCTION

Thank you, Chairman Latta, Ranking Member Castor, and members of the subcommittee. 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), a division of the North American Electric Reliability Corporation[1] (NERC), I appreciate the subcommittee's

[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 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

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 NERC and created in 1999, the E-ISAC serves as the clearinghouse for security information for the electricity industry in North 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 quality 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 1,900 member and partner organizations. E-ISAC membership represents more than 85% of the meters in North America and includes a range of utilities of all sizes and types. 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,

Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves nearly 400 million people.

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), the Department of Defense (DoD), and the Federal Bureau of Investigation (FBI). NERC also works closely with the Electricity Subsector Coordinating Council[2] (ESCC) to further partnerships that are vital to addressing security.

The E-ISAC is organizationally isolated from NERC's enforcement program to facilitate and maintain a culture of voluntary information sharing and trust. NERC and the E-ISAC adhere to a strict Code of Conduct. 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, covering a wide range of priorities and threat vectors. These include:

- Categorizing cyber systems based on impact
- Controlling electronic and physical access
- Managing system security, including malware prevention and patching
- Training personnel on security procedures

[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 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.

- Implementing plans for incident response and recovery
- Physical security protections for critical transmission substations and control centers
- Managing supply chain risks

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.

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

E-ISAC Portal – E-ISAC members and partners access information on cyber, physical, geopolitical threats, news and events through a secure Portal. Information shared with the E-ISAC is voluntary and can be shared anonymously or with attribution. The E-ISAC analyzes, enriches, curates, and shares information with the community in accordance with the Traffic Light Protocol (or TLP) system. 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 E-ISAC 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, such as the SolarWinds incident, cross-border remote access to bulk power system elements, 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. 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, national laboratories, 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 to identify additional threats based on the tools and information available. These threat hunts have helped identify additional gaps and enabled industry to apply mitigation strategies. This analysis is complemented by partnerships with cross-sector and international organizations including the Canadian Independent Electricity System Operator (IESO), Canadian Gas Association, Danish SektorCERT, Financial Services ISAC, and Oil and Natural Energy ISAC, among others. The E-ISAC also collaborates with cyber security firms to bolster information sharing and analytical capabilities, ensuring 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. 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. ETAC participants have collaborated on threats emanating from the Russian war in Ukraine, supply chain events, and operational technology vulnerabilities. ETAC is an important example of how the private sector is working with government to defend critical infrastructure.

Trainings, Briefings, and Workshops – To help industry understand the evolving threat environment and mitigations, the E-ISAC provides members and partners with regular trainings, briefings, and workshops. In addition to cyber-focused engagements, 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 on physical security to provide utilities with mitigation strategies that lead to upgrades at their facilities, thereby enhancing protective measures in defense of physical security attacks.

E-ISAC workshops teach the design basis threat methodology (DBT). 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 over 25 of these workshops since 2017 across a diverse subset of our membership. The E-ISAC will host three more workshops in 2025.

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 eighth GridEx concluded two weeks ago.

GridSecCon – GridSecCon is one of the industry's premier events that convenes hundreds of grid security experts each year from industry and government to participate for a week of training, conference, threat briefings, and networking. Participants engage in discussions on critical energy security topics such as incident response, risk management, resilience, identifying indicators of compromise, and cross-sector risk – to name a few.

CRISP, GridEx, and GridSecCon also provide opportunities for hands-on cyber security training, using realistic scenarios based off real world events.

Industry and Vendor Engagement – The E-ISAC also recognizes the increased interdependencies and complexities in the supply chain among security, vendors, and the electricity industry, and is addressing this issue through the Vendor Affiliate Program (VAP). This program brings OEM vendors and security solution providers into the E-ISAC community as partners to facilitate information sharing and best practices, leveraging subject matter expertise and thought leadership of some of the biggest suppliers to industry. VAP currently has 22 members representing manufacturers and security firms widely used by the electricity community. We expect continued growth within this community and will continue to leverage it to help mitigate the supply chain threat.

Resilient Communications – The E-ISAC is also focused on building enhanced resilience across the industry. After-action reports from previous GridEx cycles highlighted opportunities to further strengthen communication technology planning and ensure seamless coordination across

the electric sector during major events. In response to these insights, the E-ISAC, in collaboration with the ESCC Secretariat and other partners, conducted an in-depth review of the processes and tools that support the ESCC's emergency procedures. This thorough review informed the development of actionable recommendations and tools to enhance communication resilience across the sector.

The Threat Landscape

The E-ISAC is not aware of any specific, credible and imminent cyber or physical security threats to the North American electric grid at this time. The E-ISAC continues to monitor threat activity and intelligence bulletins provides stakeholders with insights into the tradecraft of politically motivated hacktivists, ransomware operators, and state-sponsored threat actors.

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, underscore 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.

As discussed further below, the E-ISAC continues to monitor threats from China, Iran, North Korea and Russia. Chinese cyber activities are 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. The sheer scale and persistence of Chinese cyber activities demonstrated in the various Typhoon campaigns lends credence to their ambition to hold North American critical infrastructure at risk. Iran's growing expertise and willingness to conduct aggressive cyber operations make it a threat to the security of U.S. and its allies, however, their regional neighbors such as Israel are more likely to experience cyber impacts. North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat, especially in the use of the thousands of cyber operatives across the world they utilize to gain access to North American critical infrastructure as remote workers. Russia remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Its focus currently remains primarily on its regional neighbors and Ukraine. Finally, the E-ISAC continues to monitor and report on physical and cyber domestic and foreign hacktivist, criminal, and ransomware threats to the sector.

People's Republic of China (PRC) Cyber Threats

Salt Typhoon is a state sponsored threat group attributed to the People's Republic of China (PRC), believed to be operated by the PRC's Ministry of State Security (MSS). They have been active since 2019 and have targeted the telecommunications, health, and hospitality sectors in the United States, Canada, and Asia. In late 2024, Salt Typhoon compromised the networks of nine U.S. telecommunications companies. In June 2025, the Canadian Centre for Cyber Security attributed Salt Typhoon to a breach at a Canadian telecommunications company in February 2025.

Salt Typhoon commonly exploited unpatched vulnerabilities in public-facing network devices including routers, firewalls, and virtual private network (VPN) solutions to gain initial access to a target network. They utilized living-off-the-land (LOTL) techniques and custom malware to go undetected for years. The activities of the Salt Typhoon extend beyond mere technical weaknesses and represent a profound strategic intelligence threat. The technologies targeted by Salt Typhoon are prolific across critical infrastructure sectors, including the electric sector, which makes repurposing tactics, techniques, and procedures learned targeting one sector easier when targeting the next.

The compromise of large data centers could lead to infiltrations in shared cloud environments and the compromise of cloud tenant data as in the case reported by NEXTGOV/FCW on June 9, 2025 where Digital Realty, a large data center operator, and Comcast report as victims of Salt Typhoon's espionage activities.[3] The service disruption and sudden disconnection of a large data center could also have impacts on grid reliability. In a report published in January of 2025, NERC identified the risks that would be present with the growth of large data center loads.[4]

Volt Typhoon was reported by Microsoft and CISA in May 2023 and has remained active since. CRISP began reporting to both DOE and the CRISP community on Volt Typhoon in October 2022, prior to public release in May 2023. This threat actor exhibits a sophisticated and stealthy

[3] See https://www.nextgov.com/cybersecurity/2025/06/us-agencies-assessed-chinese-telecom-hackers-likely-hit-data-center-and-residential-internet-providers/405920/
[4] See https://www.nerc.com/pa/rrm/ea/Documents/Incident_Review_Large_Load_Loss.pdf.

approach to cyber espionage targeting U.S. critical infrastructure. Active since mid-2021, its focus is not on immediate data exfiltration but rather on maintaining persistent access for potential future disruptions. Volt Typhoon operations leverage compromised small office/home office (SOHO) routers and network devices, often utilizing publicly known exploits for initial access. Once they have gained access, they employ extensive LOTL techniques. Additionally, they employ techniques to bypass multifactor authentication (MFA) when possible and maintain persistence through scheduled tasks or registry modifications.

The Democratic People's Republic of Korea Cyber Threat

The Democratic People's Republic of Korea (DPRK) has systematically deployed thousands of IT operatives who have applied for jobs throughout North America. The targeted jobs are designated as "remote" and are technology focused – such as Data Scientist, Software Engineer, Business Intelligence Engineer, Stack Engineer, and Data Engineer. The job roles and responsibilities usually require high-level access to include administrative access to fulfill the job requirements. The workers use fabricated personas, along with deepfakes and other artificial intelligence tools, to secure legitimate roles in IT and other technical functions.

The E-ISAC has shared numerous personas and network indicators associated with DPRK IT workers, and we have received reports from members that have received applications from these personas. The E-ISAC recommends requiring stringent background checks, implementing careful interview processes, training human resources departments to spot inconsistencies in behavior or AI deepfakes. Network security should monitor the installation of unauthorized remote administration tools and the use of VPN services to connect to corporate infrastructure.

Iranian Cyber Threats

The E-ISAC is tracking ongoing Israel-Iran tensions. Specifically, the E-ISAC continues to monitor open-source intelligence and CRISP data for any cyber activity against North American electrical infrastructure for possible retaliation of Iranian cyber actors targeting vulnerable U.S. networks and entities of interest.[5] The E-ISAC encountered upticks in activity by pro-Iran hacktivist groups claiming to carry out attacks, primarily DDoS attacks, against U.S. and Israeli organizations across numerous sectors. Though DDoS activity remains the routine standard for hacktivist activity in general, the E-ISAC continues to observe some hacktivists claiming to breach industrial control systems (ICS) in specifically targeted victim countries – most typical are pro-Russia operations targeting European sectors.

Russian Cyber Threats

We continue to monitor for Russian cyber activity in North America. Reporting suggests their cyber focus area currently remains on Ukraine and NATO affiliated countries in Europe. Russian hacktivist groups, such as NoName057(16), leveraged disruptive Denial of Service attacks to knock victim websites offline across various critical infrastructure sectors. Russian hacktivist groups can also be thought of as cyber privateers, state-sponsored actors operating as cyber criminals and geopolitical idealogues. Russian cyber actors continued their cyberespionage activity against organizations of interest to the Russian government, including in government, defense, transportation, media, non-governmental organizations, and healthcare sectors primarily in Europe and North America. We will continue to monitor this situation as Russian tactics, techniques, and procedures (TTPs) used in infrastructure in those companies could later

[5] See DHS notice: Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest.

be tailored for use against North American electric utilities.

Hacktivist, Criminal, and Ransomware Threats

Public protests have been exploited to promote violent rhetoric. For example, protests in Los Angeles resulted in several online users mentioning specific targets and tactics, such as using a specific caliber firearm against transformers and promoting "drone bombing" of a substation. The E-ISAC also observed claims of sabotage incidents targeting the electricity and broader energy sector outside of North America. For example, a series of sabotage incidents on May 24-25 in France involved downing a power pylon, an arson attack on a substation, and an arson attack on a transformer in close geographic proximity, for which two French anarchist groups claimed credit. Media attention to incidents such as these can raise visibility of various TTPs that can be used against the grid. Cyber threats focused on espionage, crime, and hacktivism will continue to evolve, led by the tensions related to the geopolitical landscape in the European, Mideast, and Asia Pacific regions.

Ransomware cyber-criminals continue to pursue common tactics that impact victims with encrypted files and assets, sensitive information exfiltrated from the victims' environment, and holding impacted technology and information for ransom while naming and shaming victims. Ransomware tactics have evolved to where groups impersonate legitimate network administrators to steal login credentials, leading to subsequent malicious activity.

Threat actors on ransomware sites and cybercrime forums monitored by the E-ISAC continue to make claims of cyberattacks against alleged energy sector victims, including energy sector

vendors, oil and gas companies, and electric utilities. Cybercrime forums often help facilitate ransomware attacks by providing platforms where threat actors can buy and sell initial/unauthorized access to victim networks, which can then be utilized for more severe follow-on attacks. Cybercrime forum activities also involve the sale or leaking of stolen data, credentials, and other illegal digital goods and services.

The E-ISAC observed a temporary drop in the number of tracked claims of cyberattacks against energy sector entities when the most prominent English-language cybercrime forum, Breach Forums, was shut down in April. However, other English-language forums seek to become a replacement for Breach Forums, and Russian-language cybercrime forums continue to operate unimpeded and now constitute all the "top-tier" forums in terms of selling or leaking victim network accesses and stolen data.

Recommendations

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

Authorize ETAC – As discussed above, DOE's ETAC pilot led by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), is a public-private partnership that convenes experts from the federal government and the U.S. energy sector, joining analytic capabilities from the national laboratories with real-world threat insights to secure critical infrastructure and support the nation's response to energy system threats. Congressional authorization of the ETAC will further establish this important partnership, enabling advancement of its important mission in collaboration

with the energy sector.

Support Funding for CRISP +30 and DOE Oil and Natural Gas (ONG) Programs – DOE's CRISP +30 and Oil and Natural Gas pilots provide critical intelligence value to both the Department of Energy and the CRISP community utility members. Begun in 2018, CRISP +30 is a DOE program supporting the participation of electricity providers with smaller customer bases, mostly cooperative and municipal utilities. A goal of the program is to facilitate participation of smaller companies that otherwise lack sufficient resources. While smaller in size, some utilities serve critical defense critical infrastructure in remote, rural areas. Their contributions are often significant. Previous funding for CRISP +30 was approximately $3 million annually, and any increase would benefit the program by adding additional defense critical energy infrastructure utilities. For example, CRISP identified and reported on malicious nation state activity attributed to Chinese nation state actors prior to publication by CISA and Microsoft. This early reporting informed DOE CESER and the sector of an emerging threat, enabling the sector to undertake proactive mitigations to better defend against new malicious cyber tactics, techniques, and procedures. Sufficient funding for the CRISP +30 expansion will enable stability and growth of this valuable partnership.

DOE'S ONG program began in 2018 in an effort to add CRISP technologies to ONG companies to increase the data set and monitor for anomalous and/or malicious activity. Maintenance or even expansion of DOE's ONG program would benefit the national security of the nation by providing cyber situational awareness to ONG participants and DOE, and providing domestic coverage of infrastructure. As malicious cyber actors continue to target ONG infrastructure, funding to maintain and potentially expand the ONG pilot would bring increased visibility and CRISP support to ONG

companies.

Reauthorize CISA 2015 – The Cybersecurity Information Sharing Act of 2015 (CISA 2015) expired on September 30, 2025, while most recently given a short-term extension to January 30, 2026. CISA 2015 was enacted to facilitate voluntary information sharing between the private sector and government. Industry sources report that the law has enhanced response capabilities to cyber incidents and meaningfully advanced information sharing and cyber defense. As a private entity, expiration of the law has no immediate negative consequences on E-ISAC operations. However, the law does encourage information sharing with ISACs and other sharing relationships. Reauthorization would support the broader information sharing ecosystem and preserve a highly valued framework for the private sector.

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. Yet the security landscape is dynamic, requiring constant vigilance and agility to help prevent and mitigate the impact of any such attacks. 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. Harmonizing reporting requirements and encouraging 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. NERC, the E-ISAC, and the industry are working 24/7 to ensure a secure and reliable grid in the face of significant threats.