

National Security Efforts in the Electric Power Sector

Electricity is vital to national and economic security, and to the life, health, and safety of all Americans.

As threats to the energy grid escalate—both from malicious actors and natural hazards—the electric power sector has answered the call to improve its security posture by working together within the sector, with other sectors, and with government partners to prepare for extraordinary events.

The Edison Electric Institute (EEI) and its member companies have made these partnerships the cornerstone of the industry's preparedness strategy, coordinating efforts among the many stakeholders responsible for keeping Americans safe and secure with access to reliable electricity.

While much progress has been made in a short time, advancing this work remains a priority. The electric power sector increasingly is seen as a model

for how critical infrastructure sectors organize to prepare for and respond to extraordinary threats, focusing on resilience, improving situational awareness, developing new tools, and working more collaboratively with a broad group of industry and government stakeholders. Further, the electric power sector plays a fundamental role in national security and has a strategic opportunity to provide a platform for resilience and key capabilities that enhance security for the sector and the nation.



Following are several key terms, organizations, and initiatives that continue to be instrumental in coordinating efforts across the sector. Many have been informed by actual events, threat briefings, the experience of engineers and operators in the electric power sector, the practices of other sectors, and the counsel of policymakers and government. They form the foundation for the sector's efforts and will continue to evolve to reflect the threats that we face today and can expect to face tomorrow.

EEL Member Company Activities Focused on Security and Resilience

Policy Committee on Reliability, Security, and Business Continuity (RSBC)

EEL's CEO Policy Committee on Reliability, Security, and Business Continuity (RSBC) develops and advances investor-owned electric companies' leadership in operational continuity and prompt power restoration. The committee also develops industry policy positions on issues concerning security and reliability and guides EEL in:

- advocacy before the federal government and other decision-making bodies;
- dialogues with key policy decision-makers and stakeholders important for continuity of service;
- external communications and education; and
- sharing of information with EEL member companies and other critical infrastructure sectors.

Seven EEL member committees report into the RSBC, providing avenues for sharing information and achieving industry objectives for senior staff with a wide range of security and reliability responsibilities.



Culture of Security Initiative

The RSBC established the Culture of Security Initiative to emphasize better understanding of, and to drive continuing improvements to, security as a fundamental component of companies' individual corporate cultures. A security culture encompasses a set of values and a sense of responsibility and behaviors, demonstrated by an organization's workforce, that contribute to the protection and safeguarding of a company's assets and operations from security threats.

Fundamentally, security is an obligation of every employee, executive, contractor, and supplier, and cannot be reserved only for a few personnel. Leadership stakeholders across a broad range of functions and activities, including operations, emergency preparedness, information technology, human resources, and communications, are essential to advancing the development of a security-conscious workforce.

The Culture of Security Initiative will identify and share practices, resources, and other tools that may be used by EEL member companies to enhance their organization's security posture and to support ongoing cultural efforts to foster employee awareness, engagement, and participation in security activities. A central component is the annual Self-Assessment Tool, which was developed to foster meaningful internal discussions on the existing maturity of each company's security culture and to help member companies assess and identify opportunities across their organizations to instill and improve a culture of security.

Fundamentally, security is an obligation of every employee, executive, contractor, and supplier, and cannot be reserved only for a few personnel.

Government-Industry Coordination

Electricity Subsector Coordinating Council (ESCC)

The CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC focuses on actions and strategies that help protect the energy grid; prevent various threats from disrupting electricity service; and develop capabilities that help the sector quickly respond and recover when major incidents impact the grid.

The ESCC includes CEOs and executives from electric companies, public power utilities, and electric cooperatives, as well as their trade association leaders. Together, they represent all segments of the electric power industry. Through the ESCC, the industry works closely with its government counterparts, including senior administration officials from the White House, cabinet agencies, federal law enforcement, and national security organizations. Canadian electric company executives also sit on the ESCC due to the cross-border nature of the North American energy grid. An EEI team, joined by its counterparts at the American Public Power Association and the National Rural Electric Cooperative Association, serves as the program manager (or Secretariat) for ESCC initiatives.

State Coordination and Outreach

In 2018, the ESCC focused on state coordination and outreach with state leaders and agencies that also are integral to preparation, response, and recovery from significant grid events. The electric power sector can leverage existing relationships and processes honed over decades of natural disaster response to tackle planning needed for response to prolonged and/or widespread cyberattacks. To that end, ESCC members are engaging with governors, state homeland security departments, public utility commissions, energy offices, and National Guard units, among others.

The Security Executive Working Group (SEWG)

The Security Executive Working Group (SEWG) brings together senior electric power sector staff from across the nation and supports the ESCC by carrying out many initiatives and projects. The ESCC Secretariat provides SEWG members regular information through monthly conference calls, a newsletter, and a private website.

Tri-Sector Executive Working Group

The ESCC worked with senior government leaders to establish the Tri-Sector Executive Working Group to advance collaboration and coordination with the Finance and Communications sectors. Senior staff from all three sectors meet regularly to develop resources, including a Tri-Sector Playbook, and to identify opportunities for collaboration, develop cross-sector risk assessments, and improve information sharing among the nation's most critical sectors.

Critical Infrastructure Protection (CIP) Standards

The introduction of mandatory CIP Standards more than 10 years ago has established a comprehensive foundation to support reliability of the bulk power (or transmission) system. These requirements have raised the security posture of the industry by setting mandatory security controls that are enforced by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the regional transmission organizations and independent system operators. The CIP Standards include more than 100 security requirements with which every electric company with an applicable system must—at a minimum—comply.

The CIP Standards, along with the initiatives and programs mentioned throughout this document, work together to address the security and reliability of the energy grid.



Information Sharing and Situational Awareness

The Electricity Information and Analysis Center (E-ISAC)

The Electricity Information and Analysis Center (E-ISAC) serves as the primary security communications channel for the industry. The E-ISAC enhances the ability to prepare for, and respond to, cyber and physical threats, vulnerabilities, and incidents in collaboration with the Department of Energy (DOE) and the ESCC. The E-ISAC gathers, analyzes, and shares security information provided by members and partners; coordinates incident management; enables member-to-member sharing; and communicates mitigation strategies with stakeholders across interdependent sectors and with government partners. Information shared with the E-ISAC is protected from FERC, NERC, and the Compliance Monitoring and Enforcement Program via signed legal agreements, NERC corporate policy, and physical and legal separation from NERC.

Cyber Analytics Tools and Techniques (CATT) 2.0™

DOE is developing Cyber Analytics Tools and Techniques (CATT) 2.0™ in collaboration with the electric power sector. The CATT concept seeks to create a platform where data gleaned from a variety of sensors on energy company systems can examine threats and events on information technology and operational technology systems. Several EEI member companies are contributing staff time and resources to industry-government discussions addressing the range of technical, legal, and policy challenges and opportunities.

Cyber Risk Information Sharing Program (CRISP)

DOE developed the Cyber Risk Information Sharing Program (CRISP) to combine state-of-the-art threat analysis capabilities with insights from the U.S.

intelligence community to identify sophisticated attacks targeting critical U.S. energy systems. CRISP analysis detects cyberattacks and threats and delivers alerts and mitigations back to owners and operators through the E-ISAC. Since 2014, the E-ISAC has managed this voluntary, subscription-based program, which now covers electric companies serving approximately 75 percent of U.S. electricity customers.

Financial Systemic Analysis and Resilience Center (FSARC).

In 2016, the CEOs of eight banks—Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo—came together proactively to identify ways to enhance the resilience of critical infrastructure underpinning the U.S. financial system. The result was formation of the Financial Systemic Analysis and Resilience Center (FSARC). Soon after, additional financial institutions, including the key financial market utilities identified as operators of essential infrastructure, joined the FSARC as member firms. The FSARC works proactively to mitigate systemic risk to the U.S. financial system from current and emerging cybersecurity threats.

Project Indigo

FSARC is exploring the potential benefits of critical sectors sharing information directly with the U.S. national security and intelligence agencies in a pilot known as Project Indigo. U.S. Cyber Command is housed in the Department of Defense, but it has an evolving mission that incorporates direct interaction with the private sector. Project Indigo has created a partnership between the FSARC and Cyber Command; in each “run” of the project, the parties have tested the sharing of expanding amounts and types of data. A small group of EEI member companies identified due to their criticality has engaged FSARC and is forming agreements for this engagement today.

Policy Organizations

National Infrastructure Advisory Council (NIAC)

The National Infrastructure Advisory Council (NIAC) is the only executive council that examines cross-sector critical infrastructure security and resilience issues and provides recommendations to the President on how to secure the nation's infrastructure. The Council includes up to 30 senior executives appointed from across the critical infrastructure sectors who volunteer their time to examine these serious issues. Members draw upon their deep experience, engage national experts, and conduct extensive research to help develop practical federal solutions for complex problems. The Council's diverse representation of owners and operators from multiple critical infrastructure sectors enables it to identify cross-sector risks and practical ways to mitigate them effectively.

The Cyberspace Solarium Commission (CSC)

The Cyberspace Solarium Commission (CSC) was created in the FY 2019 National Defense Authorization Act. The CSC is a "bipartisan effort to review the threats facing America in cyberspace and provide strategic guidance and policy recommendations on how to defend ourselves against cyber threats." The CSC features a total of 14 commissioners from Congress, federal agencies, and relevant civilian professions. It seeks to build consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences as the world enters a new phase of cyberconflict.

A key CSC effort will be developing a comprehensive cyber policy, with specific policy recommendations to implement and prioritize this approach. This work will culminate with a public report and rollout, including briefings with the congressional committees on defense, intelligence, and homeland security to discuss the CSC's findings and recommendations.

Spare Equipment Programs

Just as electric companies share crews and resources as part of the industry's voluntary mutual assistance programs to restore power, they also regularly share transformers and other equipment.

The Spare Transformer Equipment Program (STEP)

The Spare Transformer Equipment Program (STEP) provides a ready mechanism for participating entities to share assets in the event existing equipment is destroyed deliberately. Each participating electric company enters into a binding contract that provides legally enforceable rights to access hard-to-replace transformers that have been committed to STEP. STEP members commit to share specific assets in

voltage classes within which they operate. Because the equipment used to operate in each voltage class is generally interchangeable, committing these assets to STEP provides participating companies with ready access to a large pool of recovery assets that they otherwise would not be entitled to use.

More than 50 electric companies, geographically dispersed across the country and engaged in bulk power transmission services, are STEP members. STEP also underscores the importance of partnerships within the industry. Members of STEP meet regularly to administer the program, perform drill exercises, and share technical expertise.

STEP's commitment requirements are reviewed and updated annually to ensure that all voltage classes



have an adequate number of spares. The transfer of spare equipment pursuant to STEP was approved by FERC and, to the extent necessary, STEP participants secure pre-approval from their state regulators when they first join STEP. As a result, no additional regulatory approvals are necessary to access STEP's spare capacity during a presidentially declared state of emergency.

SpareConnect

SpareConnect provides an online tool for transmission asset owners and operators to connect and to share transmission and generation step-up transformers and related equipment, including bushings, fans, and auxiliary components. SpareConnect establishes a confidential, unified platform to communicate equipment needs efficiently in the event of an emergency or other non-routine failure. SpareConnect establishes an additional, trusted network of participants who are uniquely capable of providing assistance with equipment availability and technical resources.

SpareConnect provides decentralized access to points of contact that members can connect quickly with other members in affected voltage classes. Once connected, SpareConnect participants who are interested in sharing equipment work directly with each other. SpareConnect's membership currently represents the major sectors of the North American electric power industry, including U.S. investor-owned electric companies, public power utilities, electric cooperatives, federal power marketing agencies, merchant electricity generators, and Canadian public and private electric companies.

Grid Assurance & Regional Equipment Sharing and Transmission Outage Restoration (RESTORE)

In addition to these EEL-led efforts, additional spare equipment solutions have been established across the sector, including Grid Assurance—a stand-alone entity founded by five companies (American Electric Power, Berkshire Hathaway Energy U.S. Transmission, Edison Transmission, Eversource Energy, and Great Plains Energy) that offers a subscription to transmission owners to ensure access to a secure inventory of high-voltage transmission

equipment across equipment (transformer and circuit breaker) and voltage classes—as well as the Regional Equipment Sharing and Transmission Outage Restoration (RESTORE) initiative, which is designed to enhance the resiliency and reliability of the energy grid by providing additional sources for obtaining critical equipment after disasters. These projects complement many existing programs. The maturity of these industry programs led DOE to state in a March 2017 report to Congress that, “...the most efficient and effective approach [to federal spare equipment support] is one which builds on industry-based approaches and their ongoing efforts.”

The ESCC Transformer Transportation Emergency Support Guide (ESG)

The ESCC Transformer Transportation Emergency Support Guide (ESG) created by the Transformer Transportation Working Group is designed to guide the ESCC Secretariat, trade association staff, and electric company personnel on how to obtain support from government and private-sector transportation partners during incidents that require the emergency movement of Large Transmission Power Transformers (LTPTs).

The ESG supplements and supports, but does not replace, electric company logistical and transportation plans. Additionally, this guide should be used in conjunction with other industry emergency planning documents, including the ESCC Playbook, the STEP Procedures Book, the SpareConnect database, and electric power sector trade association mutual assistance plans and programs.

During an incident that requires the emergency movement of LTPTs, industry trade associations will facilitate operational-level communication and support between electric companies and public and private partners. The ESCC will provide executive-level communications, coordination, and support between the electric power industry and the federal government and private partners, as needed. These efforts will ensure that companies and our partners have:

- connectivity and updates to other industry emergency response programs;
- situational awareness about the emergency incident; and,
- channels for requests for transportation support from companies to partners, if needed.

Exercises and Mutual Assistance

Response Event (NRE)

EEL's member companies developed the National Response Event (NRE) framework to meet the challenge of supporting the restoration resource needs of members during major outages that have a national impact. EEL members identified two levels of NRE response. The critical difference between the two NRE levels is whether the event requires the national-level allocation of restoration resources due to the number of Regional Mutual Assistance Groups (RMAGs) impacted or due to resource constraints between RMAGs.

Cyber Mutual Assistance (CMA)

Building on a culture of mutual assistance and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC directed the formation of the Cyber Mutual Assistance (CMA) program. CMA is a natural extension of the electric power and natural gas industries' longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power and natural gas sectors are enhancing the ability to defend and protect against threats and to meet customers' expectations.

By coordinating with the government and providing mutual assistance to address cyber threats, the electric power and natural gas sectors are enhancing the ability to defend and protect against threats and to meet customers' expectations.

More than 155 North American electric companies, including all business models and those engaged in transport and delivery of natural gas, have joined CMA, providing valuable resources to companies serving 75 percent of U.S. customers.

Social Media Mutual Assistance (SMMA)

Given the increasing use of social media as the primary communications channel, particularly during emergencies, EEL worked with member companies to develop a Social Media Mutual Assistance (SMMA) program that is modeled after the CMA program. Through the SMMA program, EEL member companies may request assistance from other companies in maintaining effective social media monitoring, reporting, content creation, and engagement during events in which the impacted company's resource requirements are greater than it can support. Due to the nature of social media, SMMA can be provided remotely.





Research, Development, and Innovation

Supplemental Operating Strategies

While it is possible that there could be periods of operation without public or private telecommunications networks, electric companies are responsible for assessing and preparing to mitigate this vulnerability. In partnership with the North American Transmission Forum, the ESCC is pursuing Supplemental Operating Strategies (also referred to as “SOS” or “Spare Tire”), particularly the prospect of operating large parts of the energy grid without Energy Management Systems (EMS) and Supervisory Control and Data Acquisition (SCADA).

Resilient Emergency Communications

Research and development priorities have followed the initial SOS work. For example, the ESCC is focused on highlighting the critical importance of resilient emergency communications, refining the strategic framework that underpins the industry’s emergency communications plans and identifying new technologies that can fill the most critical communication gaps.

The electric power sector plays a fundamental role in national security and has a strategic opportunity to provide a platform for resilience and key capabilities that enhance security for the sector and the nation.

Electromagnetic Pulse (EMP)

The ESCC also collaborated closely with the Electric Power Research Institute (EPRI) to support its research on the potential impacts of a high-altitude electromagnetic pulse (EMP) attack on the transmission system. Research findings from this three-year research effort are summarized in the April 2019 report *High-Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies*.

The ESCC will continue to support EPRI as its research priorities evolve. New and ongoing phases of the project include: field trials in substations across the U.S. designed to provide technical expertise, support, and verification of E1 EMP hardened substation designs and development of E1 EMP mitigation asset life cycle plans; and research on the impacts of EMP on generation assets.



Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
202-508-5000 | www.eei.org



/EdisonElectricInstitute



@Edison_Electric



Edison Electric Institute

August 2019