Edison Electric INSTITUTE

Power by Association℠

Grid Security

Why It Matters

The energy grid efficiently delivers reliable and safe energy so customers always have the power they need. Protecting the energy grid is the electric power industry's top priority, and, every day, our nation's electric companies are working to improve grid security, reliability, and resiliency. In 2016, the industry was projected to invest $52.8 billion to enhance the energy grid and to further support grid security efforts.

How It Works

The electric power industry recognizes that it cannot protect all assets from all threats and instead must manage risk. The industry takes a "defense-in-depth" approach to protecting energy grid assets that includes:

- Close coordination among industry and with government partners at all levels;
- Rigorous, mandatory, and enforceable reliability regulations; and
- Efforts to prepare, respond, and recover should an incident impact the energy grid.

By working together, industry and government greatly enhance our nation's ability to defend and protect against cyber and physical security threats. The industry's security strategies constantly evolve and are closely coordinated with the federal government through a partnership called the **Electricity Subsector Coordinating Council (ESCC)**.

The 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 is comprised of the CEOs of 22 energy companies and nine major industry trade associations. This group includes all segments of the electric power industry, representing the full scope of electricity generation, transmission, and distribution in the United States and Canada.

The Role of the Federal Government

The federal government plays a crucial role in strengthening the security of the energy grid through information sharing, which includes the **Cybersecurity Risk Information Sharing Program (CRISP)**. CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders, while supporting machine-to-machine threat mitigation. Presently, more than 75 percent of all electricity customers are served by an energy company that will have deployed CRISP.

In addition to the industry-government coordination through the ESCC, security standards and regulations are important to the industry's security posture. Under Federal Energy Regulatory Commission (FERC) oversight, the electric power industry is subject to North American Electric Reliability Corporation (NERC) **Critical Infrastructure Protection (CIP) reliability standards** that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day.

Regulations and standards provide a solid foundation for strengthening the electric power industry's security posture. However, as the threat environment evolves, so must the industry's efforts.

Other Industry Actions

Energy companies plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. In November 2015, NERC conducted the third biennial, industry-wide grid security and incident response exercise, known as **GridEx III**. GridEx III brought together more than 360 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to work through incident response protocols to address widespread outages. Planning for GridEx IV in November 2017 is underway.

The electric power industry has a culture of mutual assistance based on decades of experience working together to respond to major incidents. When a weather event or natural disaster impacts a region, crews and lineworkers from all over North America descend on the affected region to restore power. Building on this long history of mutual assistance and partnership to restore power after major outages, the electric power industry is expanding equipment-sharing programs—like the **Spare Transformer Equipment Program (STEP), SpareConnect, and the newly formed Grid Assurance program**—to protect the energy grid from a range of threats and to enhance grid resilience.

As cyber risks proliferate, the industry is similarly organizing itself to pool resources in the face of incidents that exceed the capacity of individual companies to respond. The ESCC has established a **cyber mutual assistance program** to aid energy companies as they work to restore necessary computer systems in the event of a regional or national cyber incident.

Additional risks the electric power industry prepares for are **geomagnetic disturbances (GMDs) and electromagnetic pulses (EMPs)**. The industry is addressing bulk power system issues associated with GMD through the NERC-FERC standards process. Two mandatory and enforceable GMD reliability standards are on track for implementation. The ESCC is working closely with the government to better understand the threat posed to energy infrastructure from a man-made EMP, either from a high-altitude nuclear blast or a so-called “directed energy” weapon. Based on these discussions, and building on research done by the National Labs and Department of Defense, the Electric Power Research Institute is undertaking a major collaborative research effort with the Department of Energy to inform the application of technologies that will enhance energy grid resilience and accelerate recovery.

Policy Priorities

- Maintain the ESCC and government partnership.
  - Engage the Administration to align strategic priorities on critical infrastructure security and preparedness.
  - Work with the Administration on implementation of cybersecurity executive order, ensuring awareness of existing industry initiatives.
  - Drive an increased focus on response and recovery partnerships during natural disasters or threats to critical infrastructure.
- Support federal research and development on grid security technologies and expedite technology transfer to the private sector.
- Improve and expedite background checks.
  - Leverage federal law enforcement capabilities to provide enhanced background investigation screening for personnel with access to critical grid assets.
  - Coordinate more directly with law enforcement to combat insider threats.

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