Edison Electric Institute
Power By Association®

Electric Power Industry Initiatives To Protect The Nation's Grid From Cyber Threats

Protecting the nation's electric grid and ensuring a reliable supply of energy are top priorities for the electric power industry. The power grid is a complex, interconnected network of generation, transmission, distribution, control, and communication technologies, which can be damaged by natural events such as severe storms, as well as by malicious events such as cyber attacks.

Cybersecurity is not new to the electric power industry—it has been a growing priority over the past decade. The industry employs threat mitigation actions focused on preparation, prevention, response, and recovery in its operations. The electric power industry partners with federal agencies, including the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE) to improve sector-wide resilience for cyber threats. The industry also collaborates with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and federal intelligence and law enforcement agencies to strengthen its cybersecurity capabilities.

While the industry supports passage of cybersecurity legislation, it is not waiting for congressional action to enhance its cyber defenses. Instead, electric utilities proactively are forging ahead with a series of initiatives. The following are but a few recent examples of the comprehensive and ongoing activities the electric power industry is taking to safeguard the electric grid from cyber threats.

Threat Scenario Project

In 2011, the Edison Electric Institute (EEI), in conjunction with private sector experts and its member utilities, initiated the Threat Scenario Project to identify threats and practices to mitigate these threats. Identified threats included coordinated cyber attacks, as well as blended physical and cyber attacks. The project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack. The project continues to evolve as the threat landscape changes in order to keep the industry prepared to identify and defend against emerging cyber threats.

National Infrastructure Advisory Council (NIAC)

The electric power industry is closely engaged with the NIAC, a public-private council that advises the President on critical infrastructure security. In 2010, the NIAC published *A Framework for Establishing Critical Infrastructure Resilience Goals*, which recommended executive-level dialogue between the electricity sector and government leaders.

In 2012, officials from DOE, DHS, and the White House met with representatives from the major electric and nuclear sector trade associations to initiate this dialogue. Also, a classified briefing was given to more than 70 electric company CEOs on national security threats to the industry. These engagements improved CEO awareness, and resulted in the formation of a working group of CEOs, national security staff, and DOE and DHS leadership to coordinate national-level planning and preparation for response and recovery efforts before a disaster strikes.

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

In 2012, the electric power industry collaborated on a White House initiative led by DOE, in partnership with DHS, to develop the ES-C2M2 to help measure and improve the industry's cyber readiness. The model helps

electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity.

Roadmap to Achieve Energy Delivery Systems Cybersecurity

The electric power industry collaborated with DOE and DHS in 2006 to publish the *Roadmap to Secure Control Systems in the Energy Sector*, a report that was updated in 2011 to address sector changes and the evolving cyber threat. The updated report[1] outlines a strategic framework for industry, vendors, academia, and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

Electricity Subsector Cybersecurity Risk Management Process (RMP)

In 2012, electric power industry representatives helped DOE, NIST, and NERC to develop the RMP guideline to help tailor cybersecurity risk management processes to meet organizational requirements. The guideline can be used by utilities to incorporate cybersecurity risk considerations into their existing corporate risk management processes.

Mandatory, Enforceable Cybersecurity Standards

The electric and nuclear power sectors are the only critical infrastructure with mandatory and enforceable cybersecurity standards. The Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards. NERC was designated as the ERO in 2006 and worked with electric power industry experts to develop the NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009, which were approved by FERC in 2008, making them mandatory for owners and operators of the bulk electric system. Since 2008, the standards have been updated as the threat landscape continues to evolve. The Atomic Energy Act and Nuclear Regulatory Commission also have created mandatory standards for nuclear power plants.

Public-Private Information Sharing

Timely public-private information sharing is essential to help the electric power industry protect the grid against cyber threats. The industry is active in several information sharing forums, including:

- **The Electricity Sector Information Sharing and Analysis Center (ES-ISAC):** The ES-ISAC gathers industry information on security-related events for sharing with its government partners and shares government information on threats with industry.
- **The Electricity Sub-Sector Coordinating Council (ESCC):** The ESCC helps the electricity sector's owners and operators to coordinate and facilitate electric sector policy to improve the reliability and resilience of the grid.
- **DHS's National Cybersecurity and Communications Integration Center (NCCIC):** The NCCIC works with federal, state, and local governments; intelligence and law enforcement communities; and the private sector to prepare for, assess, and respond to cyber events.

As threats to the grid grow and become more sophisticated, the electric power industry remains committed to continuing to strengthen its defenses against cyber attacks.

January 2013

---

[1] *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, which is available to download at: http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf