Edison Electric Institute
Power By Association®

Electric Sector Priorities in Cybersecurity Legislation

The electric power industry is committed to protecting the nation's electric grid from cyber threats and to enhancing its cyber defenses. The power grid is a complex, interconnected network of electric generation, transmission, distribution, and communication technologies that can be damaged by natural events, such as severe storms, as well as by malicious events, such as cyber and physical attacks.

The electric sector and nuclear sector are the only critical infrastructure sectors with mandatory and enforceable cybersecurity standards. Pursuant to the Energy Policy Act of 2005, consensus industry standards are developed and established by the North American Electric Reliability Corporation (NERC), with Federal Energy Regulatory Commission (FERC) oversight and approval. These standards continue to be updated as the threat landscape evolves.

Beyond standards, the electric sector has developed close industry and government partnerships to address dynamic threats. Increasingly viewed as a model for public-private partnerships, the **Electricity Subsector Coordinating Council (ESCC)** serves as the principal forum for strategic planning among CEOs and senior government officials to improve sector-wide resilience for cyber and other grid security threats. The ESCC focuses on threat mitigation through preparation, prevention, response, and recovery.

With support from the highest levels of industry and government—including officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations—this high-level coordination has supported initiatives that improve the security posture of the industry and the nation. These include: the rapid deployment of tools used to help detect security threats; improved preparation by exercising coordinated responses to attacks on the grid; improved information sharing among government and industry stakeholders; and coordination with other critical infrastructure sectors.

Key Elements Of Effective Cybersecurity Legislation

As Congress considers cybersecurity legislation, the electric power industry supports the following goals:

- **Encourage close coordination and the sharing of information among government and industry stakeholders, including liability protections for sharing information.** Timely industry-government information sharing is essential to help the electric power industry protect the grid against cyber threats. Cybersecurity requires ongoing coordination and collaboration with those who can identify the threat—government officials—and those who can engineer solutions—the private-sector owners, users, and operators of the electric grid. The sharing of legitimate cyber threat information should not be slowed because of concerns about other matters like potential lawsuits or regulatory exposure, which is why liability protection is important.
- **Avoid conflict with, or duplication of, existing regulatory authority or standards.** Legislation should respect the electric power industry's existing regulatory structure and standards-writing process. The NERC standards process is open and transparent, and leverages the experience of industry experts. Also, FERC can—and has in some instances—require NERC to develop standards to address specific issues or vulnerabilities that may be identified.
- **Limit the scope of any new federal regulatory or enforcement authority over the electric sector to imminent threats against truly critical assets**. In times of emergency, it is important to respond quickly and in a way that might not go through the more deliberative standards-writing process. Electric utilities acknowledge that operational consequences may be necessary if there is a real, imminent threat to their

systems. However, if a vulnerability is identified and there is no evidence that it will be exploited in the immediate future, then it is more effective to develop a standard that can withstand the test of time.

- **Recognize interdependencies by including all critical infrastructure sectors in a comprehensive cybersecurity regime.** The nation's critical infrastructure sectors are highly interdependent, and cybersecurity legislation should include all of these sectors to be most effective. The electric grid cannot be considered "secure" unless the critical infrastructure the industry depends on also is protected. For example, the industry relies on telecommunications networks to operate its systems; requires water to cool its systems; utilizes transportation systems and pipelines to move its fuel; and depends on financial markets to fund its operations. Cybersecurity legislation should be comprehensive.

As threats to the grid grow and become more sophisticated, the electric power industry remains committed to strengthening its defense and resiliency against cyber attacks. Congress should enact cybersecurity legislation that helps utilities fulfill this mission.

March 2015