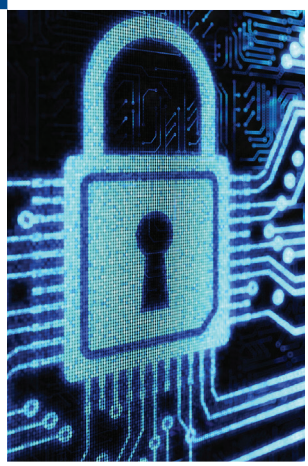
Edison Electric Institute

Frequently Asked Questions About Cybersecurity And The Electric Power Industry



Cybersecurity is an increasingly important issue, as cyber threats continue to grow and become more sophisticated. The electric power industry takes these threats very seriously. Ensuring the reliability and resiliency of the North American electric grid is our top priority, and addressing cyber threats is an important part of our reliability assurance strategy. The industry has a strong record of working together and with government partners to identify, assess, and respond to cyber threats.

The following frequently asked questions (FAQs) are designed to provide a better understanding of cybersecurity and the electric power industry's commitment to securing our nation's electric grid.

Understanding The Electric Power Industry's Regulatory Structure For Cybersecurity

■ Is the electric power industry subject to cybersecurity regulation?

Yes. Pursuant to the Energy Policy Act of 2005 (EPAct 2005), the electric power sector is subject to mandatory cybersecurity standards that fall under the jurisdiction of the Federal Energy Regulatory Commission (FERC). The electric power industry is subject to mandatory, enforceable cybersecurity standards, which help to ensure reliable operation of the electric grid.

However, we have learned that while standards enforce good business practices, standards alone are not sufficient because the cybersecurity threat environment is constantly changing, and threats and our nation's adversaries evolve rapidly. Imminent cyber threats require quick action and flexibility. Timely dissemination of threat information and analysis must play an important role in informing protective actions.

While the mandatory standards protect the electric grid against known threats, it is close coordination across the electric utility sector and with government counterparts that allows utilities to maintain a high level of reliability against new, changing and evolving threats.

■ How are the electric power industry's cybersecurity standards developed?

The North American Electric Reliability Corporation (NERC), as authorized by Congress, works with electric power industry experts, regional reliability entities, as well as state and federal government representatives to develop reliability and cybersecurity standards that apply across the North American grid, including parts of Canada and Mexico. While NERC develops the standards, FERC must review and approve them.

continued ▶

Together, NERC and FERC have a shared responsibility to ensure a reliable grid through these mandatory and enforceable standards.

To date, NERC has issued, and FERC has approved, eleven critical infrastructure protection (CIP) standards focused on cybersecurity. These standards have been revised through the NERC standards development process and have been approved by FERC five times. Currently, the electric sector must comply with Version 3 of the standards. Version 5 of these standards was approved by FERC in November 2013 with modifications and will become effective in 2016. NERC convened a standards drafting team, made up of industry subject matter experts to revise Version 5 to address FERC's required revisions. To ensure compliance, NERC conducts rigorous audits and can levy substantial fines—up to $1 million per violation per day—for non-compliance.

Wouldn't it be better—and faster—for FERC to develop the standards?

NERC's standards-drafting process has been criticized by some as being too slow and for relying too heavily on industry consensus. Yet, the current process gives FERC a substantial role in the development of the standards. In fact, FERC can direct NERC to write specific standards. Because these are technical standards affecting the operation of the grid, both NERC and FERC recognize the importance of employing the industry's operational expertise in the standards-development process. The standards-drafting process is a collaborative process that helps to ensure the cybersecurity standards are technically and operationally sound and do not result in unintended consequences.

The Electric Power Industry's Readiness And Response To Cyber Threats

When did electric utilities first begin strengthening the cybersecurity of their systems?

Electric utilities began addressing cybersecurity well before mandatory cybersecurity standards were established pursuant to EPAct 2005. In fact, the electric power industry proactively and aggressively has taken measures to mitigate cyber threats since the 1990s and the "Y2K" event; the industry continues to employ measures beyond the mandatory standards to strengthen its cybersecurity posture. Importantly, the industry remains flexible and willing to adapt as threats and the industry's systems evolve.

What are the cyber threats to the U.S. energy sector?

The energy sector faces threats to both its business-side and its operations-side. On the business-side, examples of cyber threats include data theft, denial of service attacks, Web site defacement, and customer information disclosure or privacy breaches. On the operations-side, cyber threats could target the generation and delivery of power. The greatest threat to electricity delivery is a sophisticated and coordinated cyber-physical attack on the operations-side, aimed at causing regional power outages.

What type of cyber attack could disrupt the delivery of electricity to customers?

Electric utilities take extensive measures to safeguard their systems against both operations-side and business-side attacks. However, a cyber attack on the operations-side of a utility potentially could cause electricity delivery disruptions if it can overcome the layers of defense, redundancy, and response built into the utility's operations.

The industry's mandatory CIP standards are one layer of defense aimed at protecting utility operations against cyber threats. Electric utilities also employ other defenses in their operations, including security best practices focused on preparation, prevention, response, and recovery. And, because threats rapidly evolve, utilities collaborate with government partners and each other to develop and deploy new threat mitigation actions.

What is a distributed denial of service (DDoS) attack?

A DDoS attack is aimed at making a particular machine or network service (such as online bill paying) unavailable for its intended users. In this type of attack, hundreds to thousands of compromised computer systems—including personal computers and corporate Web servers with high-speed Internet access—often are used to conduct the attack. These compromised systems are commanded by attackers to target the Web site service simultaneously. The targeted site, which is not designed to handle that much traffic all at once, slows down considerably during a DDoS attack and may even become unavailable for use by customers trying to pay bills. DDoS attacks typically are aimed at banks, credit card companies, or other online service providers.

Can a DDoS attack disrupt electricity delivery?

No. A DDoS attack is aimed at Web sites accessible and intended for use by the public. While electric utility Web sites that allow customers to pay their bills online can be targets of a DDoS attack, the networks

used by the systems that control and operate the electric grid are not connected to these billing sites and are not publicly accessible. Therefore, a DDoS attack targeted on an electric utility's billing Web site may prevent customers from paying their bills online temporarily; however, the lights will not go out.

What measures can electric utilities take to guarantee that they are secure against cyber attacks?

While electric utilities take extensive measures to secure their systems, there is no way to guarantee 100-percent security against a cyber attack because threats evolve rapidly. Utilities recognize this and build risk management, engineering resilience, and redundancy into their operations, in addition to the measures required by the mandatory cybersecurity standards.

Responding to a cyber threat requires quick action and flexibility that come only from constant vigilance and close collaboration with the government and from emergency response protocols that are planned and practiced before a disaster strikes. Utilities constantly plan for emergency situations that could impact their ability to generate and/or deliver electricity. Overall, the industry has a strong track record of maintaining high levels of reliability.

How can an electric utility determine if it is secure?

There are several tools developed jointly by the federal government and industry that help utilities measure and improve their cyber readiness. For example, in 2012, the industry collaborated on an initiative led by the U.S. Department of Energy (DOE), in partnership with the U.S. Department of Homeland Security (DHS), to develop the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The model helps utilities and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity.

How many electric utilities have been the targets of cyber attacks? What type of damage occurred as a result of the attacks?

For security purposes, we cannot share information about specific company threats or attacks. However, to date, there has not been a cyber attack on a U.S. utility that has disrupted electricity delivery. That said utilities are facing increasingly dynamic and sophisticated cyber threats from determined and well-funded adversaries, including nation states.

Who would want to attack the U.S. energy sector?

There are different groups that may have an interest in utilizing cyber attacks, including nation-states, terror cells, organized crime groups, as well as insider threats and "hacktivists"—or individuals who engage in malicious cyber activity to promote a political cause or social change.

The Role Of The Federal Government In Strengthening Cybersecurity

Why do the electric power industry and the federal government emphasize the value of information sharing?

In the fight against cyber threats, industry-government information sharing, as well as close coordination among grid operators and government partners, is critical. The federal government has the intelligence-gathering capability to identify cyber threats, while the electric power industry has the operational expertise needed to mitigate threats to the grid.

Information sharing across all critical infrastructure sectors also is a key component to cyber readiness. Electric utilities rely on telecommunications systems to operate the grid; pipelines to help fuel electricity generation; water to cool their systems and to create the steam used to generate electricity; and wholesale markets to sell electricity. Should any of these critical sectors be compromised, the electric grid could be impacted as well. Likewise, each of these sectors relies on the grid for the power it needs to operate.

How closely are federal government agencies and industry working together now?

The electric power industry partners with the White House and federal agencies—including DOE, DHS, DOD, FERC, and the FBI—to improve sector-wide resilience for cyber threats. The industry also collaborates with the National Institute of Standards and Technology (NIST) and federal intelligence and law enforcement agencies to strengthen its cybersecurity capabilities. Examples of these industry-government initiatives include:

- The National Infrastructure Advisory Council (NIAC), an industry-government council, advises the President on critical infrastructure security. NIAC recommended executive-level dialogue between the electricity sector and government leaders. This recommendation was the impetus for initial meetings in 2012 between electric power industry CEOs and senior officials from DOE, DHS, and the White House.

As a result of this initial dialogue, the Electricity Subsector Coordinating Council (ESCC) was restructured as a CEO-level group that now serves as the primary liaison between the federal government and the electric sector to address national security threats to the grid. The ESCC is focused on several key areas, including planning and exercising coordinated responses to any attacks on the grid; making sure that information about threats is communicated quickly among government and industry stakeholders; deploying government technologies on utility systems that improve situational awareness of threats to the grid; and cross-sector coordination with the other critical infrastructure sectors. Since the ESCC's restructuring in September 2013, several initiatives have been put in place to improve the industry's situational awareness and security posture.

- DOE's ES-C2M2, developed in 2012, helps electric utilities and grid operators to assess their cyber-security capabilities and to prioritize their investments to enhance cybersecurity.

The industry also partners with vendors and trade associations to improve risk management and employ mitigation actions. EEI's Threat Scenario Project, initiated in 2011 between EEI members and The Chertoff Group, is one example. The project helps security professionals and corporate leadership to evaluate their companies' strengths and weaknesses and to pinpoint areas for further improvement.

What obstacles currently are preventing federal government agencies from sharing more cyber threat information with electric utilities?

Both legal and logistical barriers can limit the sharing of cyber threat information between and among the public and private sectors. For example, the security clearance process can prevent actionable information from getting into the right hands at the right time. A strong information-sharing regime that helps to expedite security clearances and declassify threat information for use by the private sector would ensure that cyber threats are shared with entities that can help to mitigate the threats.

What type of cyber threat information would be most useful for electric utilities to have?

As a critical infrastructure, the electric power industry needs timely access to actionable threat information. Receiving a dated threat report or information that the utility cannot act upon has little value to a utility's effort to mitigate the threat. By working more closely with the defense and intelligence communities, the industry can mitigate the cyber threats that the government identifies more effectively.

What types of federal incentives do electric utilities need to enhance their cybersecurity efforts?

The electric power industry already works with government and industry partners, in the absence of federal incentives, to protect its operations. However, new incentives should support these efforts by creating opportunities to share information and to collaborate with the government, as well as allowing for flexibility in approaches and liability protections to ensure lawsuits do not threaten those who have acted in good faith.

In addition, federal legislation is needed to ensure that any information utilities provide to the government

The **Edison Electric Institute (EEI)** is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers.

With $100 billion in annual capital expenditures, the electric power industry is responsible for millions of additional jobs. Reliable, affordable, and sustainable electricity powers the economy and enhances the lives of all Americans.

EEI has 70 international electric companies as Affiliate Members, and 270 industry suppliers and related organizations as Associate Members.

Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

For more information, visit our Web site at www.eei.org.

Edison Electric Institute

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2696
202.508.5000
www.eei.org