Edison Electric Institute
Power by Association℠

EEI Principles for Cybersecurity and Critical Infrastructure Protection

Background

Protecting the nation's electric grid and ensuring a reliable supply of power are the electric power industry's top priorities. Cybersecurity incidents may disrupt the flow of power or reduce the reliability of the electric system. Key to the success of this effort is the ability to provide measures capable of protecting the evolving intelligent network against interruption, exploitation, compromise or outright attack of cyber assets, whether the attack vector is physical, cyber, or both.

The electric power industry takes cybersecurity threats very seriously. As part of the industry's overall reliability effort, electric companies work to maintain the reliability and the security of the computers, control systems, and other cyber assets that help electric companies operate the electric grid. In response to the cyber threat, electric companies employ various strategies to protect these systems, but cybersecurity threats still exist.

Addressing Cybersecurity Threats

Reliability is more than a slogan for the electric utility industry - it's a mandate. In fact, federal and state regulators have significant interest and statutory authority in ensuring electric companies provide adequate reliability. Thus, utilities take very seriously their responsibility to address cyber vulnerabilities and the security of the computers, control systems, and other cyber assets that help operate the electric grid. This focus on reliability, resiliency, and recovery takes into account an all-hazards approach, recognizing risks from natural phenomena such as hurricanes or geomagnetic disturbances to intentional cyber attacks.

Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, and the suppliers of critical electric grid systems and components. Electric companies work closely with the North American Electric Reliability Corporation (NERC) and federal agencies to enhance the cybersecurity of the bulk power system. This includes coordination with the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), as well as receiving assistance from federal intelligence and law enforcement agencies.

To complement its cybersecurity efforts and to address rapidly changing intelligence on evolving threats, the industry embraces a cooperative relationship with federal authorities to protect against situations that threaten national security or public welfare, and to prioritize the assets which need enhanced security. A well-practiced, public-private partnership utilizes all stakeholders' expertise, including the government's ability to provide clear direction and assess threats, while owners and operators of the critical infrastructure propose mitigation strategies that will avoid significant adverse consequences to utility operations or assets. At the same time a constructive regulatory environment will assure that incremental investments to protect the grid are prudent, and reduce risk in a manner proportional to the cost.

Approved by EEI Board of Directors on September 9, 2010.

Protecting the Grid is a Shared Responsibility

1. Prioritize Assets to Ensure Effective Protection

Recognizing that there are a variety of interdependencies, and potential consequences associated with the loss of different facilities, the utility industry supports a risk-based, prioritized approach that identifies assets truly critical to the reliable operation of the electric grid. This ensures the most important elements of our system receive the highest level of attention, as well as the resources necessary to secure them.

2. Threats Require Emergency Action; Vulnerabilities Should Be Addressed More Deliberately

In this context, a threat is imminent and requires a rapid response. In these instances, the industry is willing to accommodate certain operational consequences in the interest of addressing the threat. Vulnerabilities, on the other hand, have a longer time horizon and can benefit from a more measured response. Government authority should reflect and respect these different levels of danger.

3. Clear Regulatory Structure and Open Lines of Communication

The federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. It is critical that the federal government and industry communicate with each other seamlessly; to avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action.

4. Proactively Manage New Risks

As the new smart grid develops, it is essential that cybersecurity protections are incorporated into both the grid architecture and the new smart grid technologies. The electric power industry must continue to work closely with vendors, manufacturers, and government agencies and be aligned with emerging and evolving cybersecurity standards (such as those being driven by NIST) to ensure that the new technology running the grid is, most importantly, secure and reliable. We encourage the development of a security certification program that would independently test smart grid components and systems and certify that they pass security tests. This certification process would help utilities select only those systems that provide appropriate cybersecurity.

5. Committed to Protecting Bulk Electric System and Distribution Assets

The utility industry understands that cyber attacks affecting distribution systems could have broader implications. Since jurisdiction is split between state regulators and FERC, the utility industry supports enhanced threat information coordination and communication between regulatory agencies and utilities to protect our systems (whether distribution or the bulk electric system) while also honoring the existing regulatory model.

6. Cost Recovery and Liability Protection

Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.