Electric Distribution System Cybersecurity Is Critical In Today's Interconnected Society

America's electric companies are committed to providing safe, reliable, affordable, and increasingly clean energy to their customers. Protecting the nation's energy grid is essential to that mission. Electric companies constantly are evolving to keep pace with new technologies and new threats to the grid. For example, companies must keep pace with the proliferation of "smart" devices, which effectively have expanded the attack surface of the digital networks we rely on every day. As deployment of interconnected smart devices increases throughout the electric delivery system, the energy grid must be secured in new ways to prevent cybersecurity incidents from disrupting the flow of power or impacting reliability.

Electric companies continually work to protect the evolving distribution system against interruption, exploitation, compromise, or outright attack. However, companies cannot focus solely on preventing incidents. That is why the electric power industry employs "defense-in-depth" and resilience strategies that help prepare companies to restore power quickly and to continue operating in the face of all hazards.

Securing an increasingly interconnected system in a rapidly changing threat environment presents real challenges for our nation's electric companies. The industry is keeping pace, but effective policies also must be developed to address these potential safety and security risks for customers, energy grid operators, and the nation.

The Edison Electric Institute and its member companies agree that the industry's security strategies must continue to evolve to keep pace with emerging technologies and cyber threats.

To develop effective policies, the following must be taken into consideration:

- More collaboration is needed among public and private stakeholders, including energy grid operators, technology developers, policymakers, and customers to ensure national security and critical infrastructure protection are key characteristics of the evolving energy grid.
- New grid technologies represent tremendous opportunity, enabling customer choice, more efficient operations, better situational awareness, and integration of new generating capacity. The ability to operate the energy grid in a degraded state should be a part of any design plans.
- The Critical Infrastructure Protection regulatory standards have enhanced security for the bulk electric system, but the lack of homogeneity and the rapid evolution of technology make regulating security a difficult proposition at the distribution level.

New technologies and increased connectivity create new risks.

While large-scale generation and transmission systems form the backbone of the energy grid, the number of distribution assets—including distributed generation and customer devices "behind the meter"— is growing and will change the broader electricity ecosystem over time.

The growth of network-connected devices, systems, and services comprising the industrial Internet of Things (IoT) in the distribution system creates significant opportunities and benefits for society. However, the security standards of IoT devices—many of which are "consumer grade"—have not necessarily kept up with the rapid

pace of innovation and deployment. Meanwhile, as with the devices themselves, the threats from cyber actors continue to evolve rapidly.

Distribution system owners are responsible for energy grid operability and reliability, even as other parties add new distribution system components that may create new layers of associated risk.

Electric companies and their regulators take their responsibility to defend electricity delivery systems seriously. Increasing collaboration among electric companies, technology companies, and regulators is critical during the design and deployment of the energy grid to ensure visibility for grid owners and operators into these systems once they are deployed.

Assessing cybersecurity risk is especially important for new manufacturers, vendors, and service providers as they design and implement their devices, systems, and services. Security needs should be included in the design process, and initial deployments of new technologies also should be done in close coordination with incumbent system operators.

Further, distribution system owners rely on the visibility of key data and specific information to operate their systems. System operators need to ensure this data remains available when needed, has high integrity (i.e., is not altered in an unauthorized manner), and is kept confidential to ensure potential adversaries cannot exploit the information for future attacks.

As distribution owners, vendors, service providers, researchers, regulators, and policymakers seek to learn more about the distribution system's security posture, it is important to balance the needs for transparency, protection of sensitive information, and the ability to share security information in a timely manner to help distribution system owners protect their systems. This balance also must be maintained in a way that ensures the integrity of the information that operators and customers rely upon.

There are material differences between the nation's bulk electric system and more localized distribution networks, and security strategies and policymaking should reflect these differences.

The nation's generation and transmission systems make up the backbone of our energy grid. As such, a system of rigorous regulatory standards enforced by the Federal Energy Regulatory Commission (FERC) is appropriate and ensures a baseline level of security for our most critical assets. Traditionally, local distribution systems lack uniformity, are less critical to the broader ecosystem and have been regulated largely at the state level.

That said, in security, there must be priorities. While the bulk electric system has been the top priority, distribution systems supply electricity to critical customers and, because of interconnectivity, increasingly have an impact on the broader energy grid.

Thus, a collaborative, risk-based approach to security at the distribution level is essential. For example, implementing identical security measures within all distribution systems may not be feasible and could be prohibitively expensive for electric companies and their customers. Distribution system owners should balance the benefits and available resources with the risk to make informed decisions on security measures that recognize regional differences and a range of diverse threats. A risk-based approach will help electric companies assess which security measures need to be implemented in the near term and those which can be implemented over time to manage risk appropriately.

While the industry is focused on stopping cyberattacks before they happen, being prepared to respond and to recover is a key part of any security strategy.

Cybersecurity risk exists in many forms, and the potential consequences of a cybersecurity incident may vary widely. Since not all risks can be mitigated, distribution system owners must prepare to respond to and to recover from cybersecurity incidents.

The industry also is pursuing—and is uniquely capable of implementing— a system of supplemental operating strategies to ensure that system operators can maintain the flow of electricity even while operating in a degraded state. These strategies include the development of contingency plans and the ability to revert to manual operation in certain areas.

The industry's culture of mutual assistance also has expanded to include a cyber mutual assistance program that would bring industry experts together to support restoration following a cyber incident that impacts operations. Participation continues to grow, and more than 80 percent of all customers in the United States are served by electric companies that are members of the program.

Protection of critical infrastructure is a responsibility shared by industry operators, government policymakers, technology providers, and the national security community.

Information sharing among distribution owners, operators, vendors, service providers, and government agencies regarding threat and vulnerability identification and monitoring, incidents, responses, and recovery efforts is needed to prevent cybersecurity incidents from spreading.

This is crucial for managing cybersecurity risks that may be present in hardware, software, or third-party services. Addressing supply chain security is a challenge facing the nation and all critical infrastructure providers, but is a priority that is integral to the protection of cyber systems deployed throughout the energy grid.

There is no question that smart technologies are creating new risks, but the electric power industry has been, and remains, committed to developing the security, mitigation, and response strategies needed to ensure energy grid security and resiliency. No one electric company or set of standards can do this all alone, which is why the industry also is committed to maintaining and to growing partnerships across the industry and with the government to protect our nation's critical infrastructure and to deliver the security and reliability our customers expect.

April 2018