MEET the THREAT

# *States Confront the Cyber Challenge*

**Cybersecurity and Critical Infrastructure**
**October 25th, 2016**

## The Threat to Critical Infrastructure

Modern society depends on critical infrastructure facilities, such as transportation networks, telecommunications lines, water mains, and power lines, which are central not only to daily life, but also to national security. Each of these sectors increasingly uses integrated computer networks to link widely dispersed facilities and corporate offices, control equipment remotely, and meet customer demand for affordable service. For various reasons, many of these systems are vulnerable to compromise, but cybersecurity in these industries is largely a voluntary exercise. Certain sectors have expanded the number of attack vectors by introducing more Internet-connected devices and automating further functions. As a result, large swaths of the nation's electric grid, water supplies, and logistics nodes remain subject to possible disruption by foreign adversaries. In addition, relatively unsophisticated criminals can take advantage of widely available software tools that can help launch advanced cyber attacks of a kind that once originated exclusively from nation states.

## Ongoing Challenges to Improving Security

*Convenience*: When utilities first introduced digital industrial systems, security relied on physical isolation; critical systems could be manipulated only through physical interfaces. In recent years, many utilities have used the Internet to connect once-isolated systems to geographically-disperse assets and corporate offices. While the ability to monitor and control industrial systems from anywhere has lowered costs, these innovations inevitably introduce security vulnerabilities.

*Private ownership of public assets*: Most critical infrastructure is operated by private companies. Yet because they deliver a public good, their cybersecurity measures are a matter of public policy.

*Lack of information sharing*: Many utilities and public utility commissions do not receive timely threat intelligence, often because their personnel lack security clearances.

*Little experience with cybersecurity failures*: Critical infrastructure operators and emergency managers are well-versed in responding to natural hazards of the kind that cause short-term blackouts. But these individuals have little experience assessing or responding to cyber threats that can create different obstacles to restoring business operations.

*No defense in depth*: Some critical infrastructure systems rely on a single security product, such as a firewall, to defend against attacks, without comprehensive security measures that extend throughout a network.

## Recommended Steps for Governors

*Work with other Governors and lawmakers to evaluate costs and benefits of regulation*: Most conversations about cybersecurity in critical infrastructure inevitably turn to the question of incentives and regulation. Some experts believe that government should provide incentives to encourage utilities to implement best practices in cybersecurity. Others argue that the high costs for security upgrades mean utilities will never adhere to proper security standards without government mandates. Governors should work with one another, as well as state and federal lawmakers, to weigh the various considerations and determine what regulations, if any, make sense.

*Institutionalize regular contacts between relevant officials and state utilities*: Governors should ensure that homeland security advisors and public safety directors maintain working relationships with all leaders of state utilities. In the event of a significant cyber incident that affects critical infrastructure, these relationships will prove critical in properly managing any resulting crises and restoring normal operations.

*Audit existing rules and practices*: State agencies and utility commissions already regulate critical infrastructure in a variety of ways. States should evaluate if and how existing rules address cybersecurity, and whether utilities are in compliance, and whether additional standards are prudent.

*Focus on resiliency*: Because instituting strong cybersecurity in all utilities—either through voluntary measures or regulatory action—will take many years, Governors should ensure that state policy prioritizes resiliency. Governors should assume they will suffer an incident, and adapt existing response and recovery measures to cybersecurity. Governors should also convene cross-sector partners to ensure that utilities have what *they* need to be resilient, e.g., engineer graduates with the skills needed to operate critical systems manually.

*Explore public private partnerships between state regulators and the private sector*: Private companies throughout the United States employ world-class experts in infrastructure and information security. Governors should work with industry leaders to use this pool of talent to ease the burden on state regulators tasked with assessing utilities' compliance with security standards.

*Ensure that all stakeholders are involved*: Many high-level discussions about cybersecurity in critical infrastructure leave out key participants. For example, hundreds of small, non-profit electric cooperatives serve millions of Americans across the United States, and most cannot dedicate sufficient resources to cybersecurity. Governors should ensure that any statewide cybersecurity initiatives or plans account for all utilities, and not limit public-private partnerships to the largest, publicly-owned companies.

*Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at:* tblute@nga.org *with any questions.*