Issue Snapshot: Cybersecurity

Background: As an operator of critical energy infrastructure, Con Edison recognizes first hand that it faces a heightened risk of cyber attack, and has an inherent interest in protecting its assets. Con Edison operates a system that goes above and beyond current standards

Con Edison has adopted a formal cyber security policy based on the International Standards Organization (ISO) 27001 standard. The program has continued to evolve over the past years by adopting best practices developed through external interaction and participation with security vendors, benchmarking groups, Department of Energy (DOE), Department of Homeland Security (DHS), North American Electric Reliability Corporation (NERC), the Edison Electric Institute (EEI) , the American Gas Association (AGA), and federal law enforcement organizations.

In addition to government collaboration, Con Edison has been engaged in several industry led initiatives including the Threat Scenario Project with the help of EEI and The Chertoff Group. This project was designed to systematically examine a range of threats for which EEI member companies should be prepared. The resulting product is a self-assessment tool for utilities to review and understand the wide range of threats that could impact operations while identifying industry best practices to mitigate common vulnerabilities.

Company Position: After the U.S. Congress failed to act on cyber security legislation, the White House began pursuing its own policy changes. On February 12, 2013, President Obama issued a Cybersecurity Executive Order (EO).

The scope of the Order is narrow and focused on improved public-private coordination with some direction to regulators to "use all existing authority" to address cybersecurity for the industries they regulate.

The order directed the National Institute of Standards and Technology (NIST) to develop a "cybersecurity framework" (best practices or standards) for critical infrastructure. Stakeholders actively assisted in developing the framework and it became available in early 2014.

While standards are an important component to cyber preparedness, the dynamic nature of cyber threats requires more than rigid compliance checklists. Additionally, any federal standards must not conflict with or duplicate existing regulatory structures at NERC or the New York Public Service Commission.

Furthermore, although the EO includes identified incentives for compliance with the new standards, many of these require congressional action. For example, there are currently no liability and information security provisions for companies that share threat information with each other or with the federal government and vice versa.

Con Edison will continue working with Congress to ensure a robust threat information sharing program is included in any cyber security legislation.