ELECTRIC GRID SECURITY: A COORDINATED EFFORT? OR A CONFUSING PATCHWORK?

For individual utilities looking for a single, centralized source of comprehensive and authoritative information on physical and cyber security, there doesn't seem to be one. There are almost a dozen federal agencies involved; several industry organizations; a number of specially-created councils, programs, and centers, many of which are public-private partnerships; and numerous "field exercises" being coordinated by multiple agencies.

For starters, the electric power industry partners with federal agencies, including the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE) to improve sector-wide resilience for security threats. The industry also collaborates with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and federal intelligence and law enforcement agencies to strengthen its security capabilities.

There are also several specially-created entities working on various aspects of grid security, which also are tasked with disseminating information on grid security to interested parties:

- One is the National Infrastructure Advisory Council (NIAC), a public-private council that is set up to advise the President on critical infrastructure security.

- Another is the Electricity Subsector Coordinating Council (ESCC), which serves as the principal liaison between the electric sector and the federal government for coordinating efforts to prepare for, and respond to, national level disasters or threats to critical infrastructure. Electric company CEOs, as well as senior administration officials from the DOE, the DHS, the FBI, and the White House meet on a regular basis to focus on three primary grid security areas: tools and technology, information flow, and incident response. Specific initiatives focus on mutual assistance programs, cyber mutual assistance, and spare equipment programs.

- Another is the Electric Sector Information Sharing and Analysis Center (ES-ISAC), which gathers industry information on security-related events for sharing with its government partners, and also shares government information on threats with the electric industry.

- Another is DHS's National Cyber and Communication Integration Center (NCCIC), which works with federal, state and local governments; intelligence and law enforcement communities; and the private sector to prepare for, assess, and respond to cyber events.

- Another is the Cyber Risk Information Sharing Program (CRISP), also a public-private partnership co-funded by the DOE and industry. CRISP seeks to facilitate timely bi-directional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry.

In November 2015, NERC, in cooperation with the DOE, DHS, DOD, and the FBI, along with approximately 10,000 other individuals representing 350 utilities and other organizations, engaged in a two-day Grid Security Exercise III (GridEx III), the third in a series of grid security initiatives designed to address physical and cyber security issues related to the nation's electric grid.

In April 2016, the Department of Energy convened 200 participants from the oil and gas and electric power industries, as well as federal and state officials, in an effort called Clear Path IV, to test response and restoration protocols to a catastrophic simulated earthquake and tsunami in the Pacific Northwest.

In June 2016, the Federal Emergency Management Association (FEMA) engaged in a three day exercise called Cascadia Rising, which was set up to test first responders and government emergency personnel responses in the immediate aftermath of a significant earthquake.

Also in June 2016, the Department of Defense and the National Security Agency (NSA) engaged in a two-day exercise, called Cyber Guard, that tested the response capabilities of 1,000 energy, IT, transportation, and government experts to a major cyber attack.

Besides a massive number of agencies and other entities working on physical and cybersecurity, standards in this area continue to be moving targets.

In July 2016, for example, FERC directed NERC to develop an improved cybersecurity protocol to protect the nation's electric grid, including the introduction of a supply chain risk management standard designed to protect both information systems and related bulk electric system assets. In specific, FERC directed NERC to develop a "forward-looking, objective-based" reliability standard that requires security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.

In addition, FERC is considering changing the Critical Infrastructure Protection (CIP) standards related to the protection of control centers that are used to monitor and control the bulk electric system in real-time.

Also in July, the Department of Energy announced $15 million in new funding to the National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) - to be split equally between the two entities, to strengthen and protect the nation's electric grid from cyber and physical attacks.

ELECTRIC GRID SECURITY: A COORDINATED EFFORT? OR A CONFUSING PATCHWORK?

The funding is part of a $210 million (to date) funding stream that began in 2011, through DOE's Office of Electricity Delivery and Energy Reliability's Cybersecurity for Energy Delivery Systems (CEDS) program.

"As our definition of energy security and the cyber threat landscape evolve, we continue to help our partners strengthen the ways in which they protect critical infrastructure," said Dr. Elizabeth Sherwood-Randall, U.S. Deputy Secretary of Energy, during the announcement of the funding. "This funding is another important step in improving the resiliency of our power grid and our ability to respond quickly and effectively to threats in today's dynamic environment."

Over the next three years, NRECA and APPA will use the funding to develop security tools, educational resources, updated guidelines, and training on common strategies that can be used by their members to cultivate and improved cyber and physical security culture. Activities designed to bolster the members' security capabilities will include exercises, utility site assessments, and a comprehensive range of information-sharing.

In response to the funding announcement, the NRECA noted that: "Cooperatives will assess their cybersecurity programs, identify and address priorities, test strengths and weaknesses of existing systems, integrate new technologies, and share information that will enable to utility sector as a whole to build on lessons learned."

Sue Kelly, president and CEO of the APPA, noted that, "Obviously, their (APPA members') approach to cyber security and their needs and the threats that face them are different, so each one has to kind of have an individually tailored approach."

So, how should utilities get started with security efforts? And where should they turn when they want information on physical and cyber security, as well as information on the latest standards and funding opportunities?

These days, the more effective cybersecurity measures are not those that are preventive, but those that involve recognition and containment. There will always be someone who is capable of cracking a utility's security wall and finding a way in. So, an important approach is early detection and recognition, followed by quick efforts to contain it and/or shut it down, such as healing and redirection.

The same is true on the physical security side. Utilities are often very exposed and vulnerable in terms of physical assets, so the question is, "Where do you start?" Again, while it is important to take basic steps to try to prevent attacks on physical assets, a lot of effort needs to be focused on early detection, recognition and containment, such as redundancy. Again, it is difficult to prevent attacks, because you never know what someone is capable of in terms of a physical attack until they reveal it, and then it is too late to prevent it.

Each utility's needs are different, and experts at Finley Engineering can discuss your specific needs and help you select the right direction to head when it comes to security issues.

About The Author

Phil Carroll, Vice President of the Energy Group for Finley Engineering, has been involved in the electric utility industry for the past 21 years. Managing multi-million dollar projects around the country, Carroll has been responsible for the design of distribution and transmission lines, material specifications, contract administration, final acceptance, and close-outs. He is also a registered Professional Engineer in the states of Nebraska, Oklahoma, Texas, Washington, Oregon, California, New Mexico, Nevada and Arizona.

For more information, you can contact Phil at p.carroll@fecinc.com or 417-682-5531.