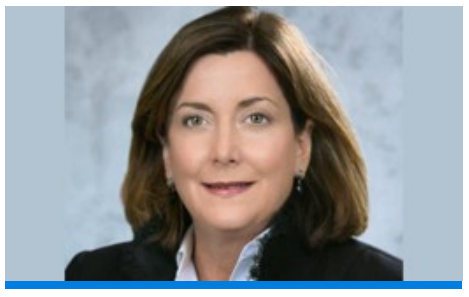
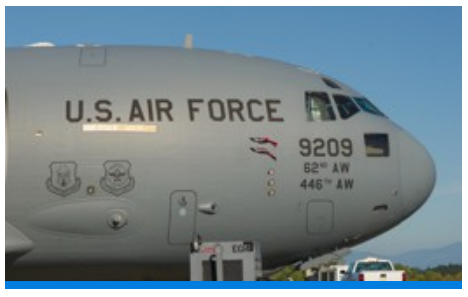
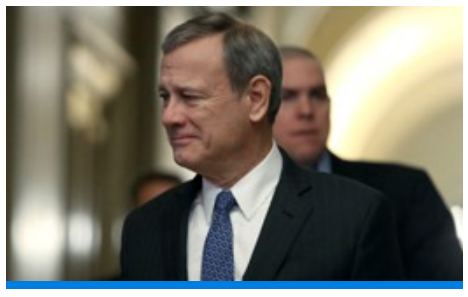
CACI Secures $514M Army Contract For Fiber-Based High-Speed Communications



PROJECT 38: New Maximus Federal Leader Forges The Path Forward



M&A Concerns Nix $280M Contract Award



Supreme Court Hearing Turns To The Contractor Mandate

Search... Go

Electric industry creates alternative channel for sharing data on infrastructure security

By WILLIAM JACKSON // AUGUST 11, 2009

EnergySec has grown to include 200 members from the electric power industry, security vendors and government regulators since its formation in December to provide an alternative to the more formal ISAC for rapid sharing of information.

COMMUNICATIONS AND NETWORKING CYBERSECURITY

IT INFRASTRUCTURE - TELECOM SECURITY

Sharing information in the energy sector should be easy because the grid is operated as a utility rather than a competitive commercial enterprise, according to EnergySec director Seth Bromberger.

Operators of the nation's power grid have joined with government regulators and security vendors to create forum for sharing information about threats to the U.S. energy infrastructure.

The Energy Sector Security Consortium (EnergySec) has grown from an informal regional industry group in the Pacific Northwest to include more than 200 members since its launch as a national organization in December 2008. Its goal is to provide a channel for sharing security information and concerns in a way that is faster and more flexible than existing organizations.

"There is no competitive disadvantage" to sharing information, Bromberger said. "Ultimately, the infrastructure is owned by one group. If we can't make it work in the energy sector, it's not likely going to work anywhere else. This is the low hanging fruit."

But exchanging data through the traditional channel, the Electricity Sector-Information Sharing and Analysis Center (ES-ISAC), is complicated because the ES-ISAC is managed by the North American Electric Reliability Corporation (NERC), the industry's designated international self-regulatory authority. That gives ES-ISAC a formal role in enforcing the Critical Infrastructure Protection Standards for the industry's bulk electric power distribution system.

"Most utilities have very strict rules of engagement when it comes to the regulators," Bromberger said. "So sharing information with them can pose some challenges. That requires a big vetting action."

EnergySec works closely with the ES-ISAC, Bromberger said, but is intended to provide an alternate channel to facilitate the flow of information in a less formal environment.

As the power grid becomes more automated and its control systems are networked on a large scale, the security of the system has become a critical issue, especially with the development of a new interactive smart grid and with recent reports that the current grid has been compromised by hackers. Current industry security standards require "the identification of and documentation of the critical cyber assets associated with the critical assets that support the reliable operation of the bulk electric system," using a risk-based assessment. Violators can be fined as much as $1 million a day. Audits for compliance with the Critical Infrastructure Protection Standards began last month.

The Federal Energy Regulatory Commission is the government overseer of the U.S. power grid under the Energy Policy Act of 2005, but the audits are carried out by NERC. Despite FERC's authority, there is still a high degree of self-regulation in the power system. NERC developed the security standards, which FERC approved earlier this year.

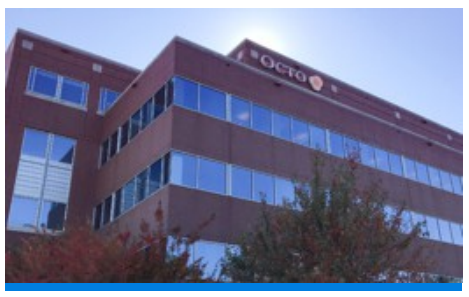
EnergySec began life as E-Sec NW, a group of electric utility security officials in the Pacific Northwest that met at lunch to share information. After winning the SANS Institute's National Cybersecurity Leadership Award in 2007, the group gained visibility and new members from around the nation, leading it to incorporate as a national nonprofit organization in December. Organizers had hoped to reach the 200-member mark by June 2010, but have reached that mark 10 months early.

The group operates a secure Web portal for sharing information and concerns, and seeking information. Some of the industry still is struggling to understand the new Critical Infrastructure Protection Standards, and the ability to ask questions about without attribution has been a valuable tool in evaluating and understanding the requirements, Bromberger said. The site also can provide near-real-time security alerts and situational awareness from information reported by members. Members can receive alerts and RSS feeds of data from the site.

EnergySec also has outreach and educational activities and is hosting a national conference in September in Seattle. Information about the conference and about the organization is available at www.energysec.org.

NEXT STORY: Serco wins immigration services contract

Batsakis, Speigel Move Quickly On Another Acquisition



How Octo's B3 Group Acquisition Drives Its 'At Scale' Ambitions

Peraton Can Claim $343M TSA IT Recompete Win

Why A National Cyber Academy Is A Bad Idea