
Diane T. Hooie

Deputy Assistant Secretary & Director for the National Cyber Security Division

Energy delivery systems are critical to the effective and reliable operation of North America’s energy infrastructure (electric power generation, oil, and natural gas production, transmission, and distribution systems) provides energy for our way of life. Today’s highly reliable and flexible energy infrastructure is only possible because of the energy delivery systems’ ability to provide timely information to system operators and automated control over a large, dispersed network of assets and components. This vast and distributed control requires energy delivery systems to communicate with thousands of nodes and devices across multiple domains, exposing energy systems and other dependent infrastructures to potential harm from accidental and malevolent cyber attacks.

Cybersecurity is a serious security challenge for the energy sector. Energy control systems are uniquely designed and operated to control real-time physical processes that deliver continuous and reliable power to support national and economic security. As such, they require security solutions that meet unique performance requirements, design, and operational needs. Cyber threats to energy delivery systems can impact national security, public safety, and our economy. Because the private sector owns and operates most of the energy sector’s critical assets and the Federal government is tasked with national security, securing North America’s energy delivery systems against cyber threats cannot be achieved by either the private or public sector working alone. Cybersecurity is a shared responsibility between the public and private sector.

The Department of Energy (DOE) is working to modernize the energy sector and integrate secure control systems. A common vision and framework for achieving this vision has been developed to guide the public-private partnerships that will secure energy delivery systems. This common vision, from the Roadmap to Secure Energy Delivery Systems, is that within ten years resilient energy delivery systems will be designed, installed, operated, and maintained to survive a cyber incident with no loss of critical function. The DOE Office of Electricity Delivery and Energy Reliability, Cybersecurity for Energy Delivery System (CEDS) Program, has implemented a multi-faceted program to address long-, mid-, and near term research, development, and implementation to meet the stringent cybersecurity requirements of the energy sector. The approach to addressing the cybersecurity needs of the energy sector that is being addressed through the CEDS Program and their public-private partnerships will be discussed.