Deep Dive

Federal Cybersecurity Resources

The U.S. Department of Energy leads the coordination of other federal agencies and private sector entities to develop guidance related to the management of cybersecurity risks in the energy sector.

The following are some of the tools available to electric utilities seeking to address cybersecurity risks:

National Cyber Alert System **(U.S. Department of Homeland Security)**

Subscribe to the National Cyber Alert System to receive free, timely alerts on new threats and learn how to protect your area of cyberspace.

Electricity Information Sharing and Analysis Center

The Electricity Information Sharing and Analysis Center is operated by the North American Electric Reliability Corporation and hosts an online portal for sharing: cybersecurity information; NERC alerts; cybersecurity incident bulletins and reports; information about exercises and conferences; and analytical capabilities. Membership is free and electric sector asset owners and operators can register for a portal acount online at www.eisac.com.

Cybersecurity Capability Maturity Model **(U.S. Department of Energy)**

The Cybersecurity Capability Maturity Model (C2M2) is used to assess an organization’s cybersecurity capabilities and prioritize the organization’s actions and investments to improve cybersecurity. There is an electric sector-specific version of the C2M2.

Cyber Resilience Review **(U.S. Department of Homeland Security)**

A self-assessment tool designed for an organization to evaluate its operational resilience and cybersecurity practices across ten domains.

Cyber Security Evaluation Tool **(U.S. Department of Homeland Security)**

A tool developed by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), now an integral component of the Cyber and Infrastructure Security Agency within the Department of Homeland Security, to assist organizations in protecting key national cyber assets. The tool provides users with a systematic and replicable approach to assessing the cybersecurity of its information systems and networks.

Risk Management Process Guidelines **(U.S. Department of Energy)**

The USDOE’s Office of Cybersecurity, Energy Security, and Emergency Response is responsible for the development and maintenace of the Electricity Subsector Cybersecurity Risk Management Process guidelines, which are intended to enable electric system operators to apply effective and efficient cybersecurity risk management processes.

Meanwhile, there are also important cybersecurity standards that have been developed nationally for the electric sector:

Critical Infrastructure Protection Standards

The North American Electric Reliabilty Corporation's Critical Infrastructure Protection Standards establish regulatory requirements to assist in securing the assets that operate and maintain the bulk electric grid.

Guidelines for Smart Grid Cybersecurity **(National Institute of Standards and Technology)**

The National Institute of Standards and Technology published Interagency Report (IR) 7628 to present an analytical framework to develop effective cybersecurity strategies designed specifically for smart grid-related characteristics, risks, and vulnerabilities.

OREGON
DEPARTMENT OF
ENERGY

This Deep Dive is part of the *Oregon Guidebook for Local Energy Resilience: For Small and Medium Utilities*, first published in June 2019.

www.oregon.gov/energy | askenergy@oregon.gov | 503-378-4040