FEMP
Federal Energy Management Program

Cyber-securing Facility Related Control Systems

The U.S. Federal government executes a wide variety of unique and challenging missions, including safeguarding national critical infrastructure, conducting scientific research, engaging in diplomacy, and providing benefits and services for the American people.[1] These missions must be executed effectively and without disruption from malicious cyber activities.

Federal facilities are increasingly equipped with control systems that use information technology to ensure the safety and comfort of occupants, enhance efficiency, lower facility costs, and optimize operations. These facility-related control systems are automated, networked, and connected to other information systems and, in some cases, to the internet. Federal facilities are also increasingly leveraging on-site distributed energy resources that require connections to outside networks or the internet.

Historically, the obscurity of proprietary operational technology (OT) systems and physical isolation from the outside world provided adequate protection. Today, increased connectivity requires diligence to secure these OT systems from cyber intrusions and attacks.

This fact sheet describes some of the tools and resources available from the Federal Energy Management Program to help federal facilities increase their cybersecurity. It also outlines the key federal regulations, guidance, and standards for cyber security (see Table 1).

Table 1 - FRCS Cyber Security Drivers

Laws and Regulations	Federal Information Security Modernization Act of 2014 (FISMA)
	IoT Cybersecurity Improvement Act of 2020
	Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)
	Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)
	Executive Order 13870: America's Cybersecurity Workforce (May 2019)
	Executive Order 14028: Improving the Nation's Cybersecurity (May 2021)
	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
	Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
National Institute of Standards and Technology (NIST) Standards and Guidance	NIST Special Publication (SP) 800-18 Rev 1: Guide for Developing Security for Federal Information Systems (Feb 2006)
	NIST SP 800-37 Rev 2: Guide for Applying the Risk Management Framework to Federal Information Systems (Dec 2018)
	NIST SP 800-53 Rev 5: Recommended Security Controls for Federal Information Systems and Organizations (Sept 2020)
	NIST SP 800-82 Rev 3: Guide to Operational Technology (OT) Security (Sept 2023)
	NIST SP 800-115: Technical Guide to Information Security Testing and Assessment (Sept 2008)
	NIST SP 800-184: Guide for Cyber Security Event Recovery (Dec 2016)
	NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government (Nov 2021)
	NIST Cybersecurity Framework (CSF), developed from EO 13636
Other Standards	ANSI/ISA/IEC-62443-2-1 (99.02.01)-2009: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
	Cybersecurity Maturity Model Certification (CMMC) (Department of Defense)

[1] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

FEMP tools and resources for cybersecurity

The Federal Energy Management Program (FEMP) helps federal facilities enhance their cybersecurity posture via tools, information resources, training, technical assistance, and stakeholder engagement. FEMP tools include free self-assessment tools that can help identify potential cybersecurity risks. FEMP focuses on operational technology (OT) cybersecurity risk. OT is hardware and software that can detect or cause a change through direct monitoring and/or controlling physical equipment, devices, processes, and events. If compromised, OT technologies could have both cyber and physical impacts. With increasing connectivity between the digital and physical worlds, the risk of exposing essential systems to disruption grows. As facilities move from analog systems to connected OT, the possibility of a disruptive cyberattack grows, requiring facilities to increasingly assess and enhance their cybersecurity posture.

Distributed energy cybersecurity

The Distributed Energy Resource Cybersecurity Framework (DER-CF) helps pinpoint cybersecurity vulnerabilities for renewable energy systems and develop customized action plans to improve security controls and practices.

The Distributed Energy Resource Risk Manager (DER-RM) lightens the workload for organizations by streamlining and managing the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) process in an easy-to-use, downloadable application. The DER-RM is an extension of the National Renewable Energy Laboratory's DER-CF and specifically focuses on NIST-RMF compliance—a major undertaking for federal sites and a critical framework for secure operations.

Facility related control systems cybersecurity

The Facility Cybersecurity Framework (FCF) helps facility owners and operators manage their cyber security risks in their OT and Information Technology networks. The FCF has a suite of free self-assessment tools tailored for the facility context that can help identify needs, find gaps, understand and mitigate gaps, and enhance cybersecurity knowledge.

Users can identify key priorities from facility and site management to inform how to assess, mitigate, and track your facility's cybersecurity posture over time by leveraging the Management Priorities tool to define goals for each NIST domain. Use the FCF core assessment tool to assess your cybersecurity policies against the NIST Cybersecurity Framework to comply with Executive Order 13686 and 13800. Or if your site uses NIST RMF, use the RMF Pre-Assessment tool for guidance on how to implement security controls based on the identified baseline, focusing on the Select and Implement steps of the RMF to help prepare for the RMF process before the implementation of controls.

After completing an FCF assessment, the Management Priorities & FCF Comparison functionality allows users to see the difference between your vision and the current state of your facility, allowing you to identify a potential mitigation path towards meeting your goals. Or use the Best Practices tool to understand how identified gaps from the FCF assessment could be exploited by known OT cyberattack techniques and tactics.

Conclusion

Addressing cybersecurity concerns will help reduce risk from connected technologies that offer potential energy, water, and emissions savings – or operations improvements that result in increased occupant comfort or maintenance benefits.

Contact:
Jason Koman
Jason.Koman@hq.doe.gov

FEMP
Federal Energy Management Program

For more information, visit:
energy.gov/femp

DOE/FEMP- 0016