U.S. DEPARTMENT OF
ENERGY
Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

Energy Management Information Systems Cybersecurity Best Practices

Energy Management Information Systems (EMIS) are a broad and rapidly evolving family of tools that monitor, analyze, and control building energy use and building/metering system performance.[1] All EMIS scope systems—such as building automation systems, geographic information systems, distributed energy resources, and automated or advanced metering infrastructure (AMI)—must be securely connected to the EMIS and must not open vulnerable pathways to other facility networks and operations. This best practices fact sheet provides an overview of required standards for EMIS cybersecurity compliance and authority to operate along with additional recommendations.

Cybersecurity for EMIS Scope Systems

Critical facility systems are often integrated with or operate on the same networks as EMIS scope systems, necessitating stable, continuous, and secure communications. When connecting EMIS to building automation and utility control systems, there are also many physical assets that could cause harm to the building and its occupants if a malicious act or human error were introduced.[2]

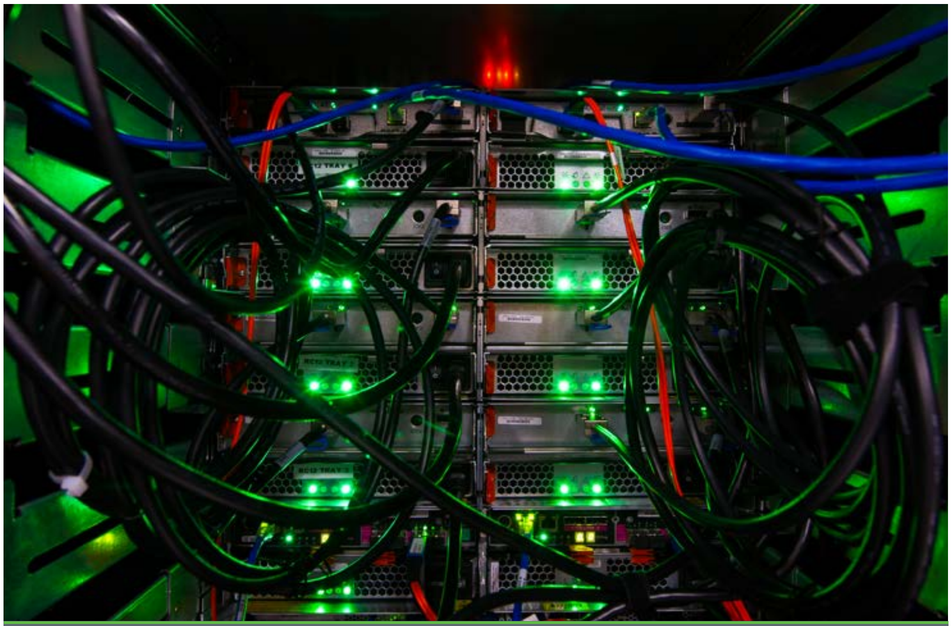

Figure 1. Cybersecurity is a critical part of planning an EMIS implementation. *Photo by Dennis Schroeder, NREL 24586*

Cybersecurity challenges arise when EMIS scope systems do not have clear boundaries and defined interconnection points for information exchange. Legacy equipment within the AMI, for example, communicates with photovoltaic arrays and inverters using protocols such as Modbus, which are inherently insecure. The following high-level cybersecurity best practices support secure integration and cybersecurity compliance for the EMIS scope systems:

- **Information security**—Secure the communications and protocols using user authentication, encryption, offline backups, and certificate management mechanisms.
- **Network security**—Implement network segmentation, perimeter control, event logging and monitoring, baselining, and physical security for legacy equipment.
- **Access control**—Ensure least privilege to a variety of users using access control lists, passwords, two-factor authentication, and role-based access control.
- **System hardening**—Limit attack surfaces by defining requirements, such as including security within the procurement process and secure patch management.

Federal Cybersecurity Requirements

As part of the EMIS planning process, each federal agency should include a description of how federal cybersecurity frameworks and requirements will be applied to secure its EMIS.

Federal Information Security Modernization Act

The Federal Information Security Modernization Act (FISMA) of 2014 requires federal agencies to implement a security program to manage organizational risk and ensure the agency-wide security of information and information systems, including agency-owned assets as well as those provided or managed by another agency or contractor. Like AMI, as depicted in the upcoming revised Federal Building Metering Guidance per the Energy Act of 2020, an EMIS is considered to be an information

[1] U.S. Department of Energy. 2015. *A Primer on Organizational Use of Energy Management and Information Systems (EMIS)*. Berkeley, CA: Lawrence Berkeley National Laboratory. https://betterbuildingssolutioncenter.energy.gov/sites/default/files/attachments/EMIS_Primer_Organizational_Use.pdf.

[2] Cutler, Dylan, Stephen Frank, Michelle Slovensky, Michael Sheppy, and Anya Petersen. 2016. "Creating an Energy Intelligent Campus: Data Integration Challenges and Solutions at a Large Research Campus." ACEEE Summer Study on Energy Efficiency in Buildings. https://aceee.org/files/proceedings/2016/data/papers/12_1016.pdf.

system. To agencies that fall under this requirement, EMIS-scope systems that may be integrated into the EMIS and related assets that collect, process, store, maintain, use, share, disseminate, and dispose of information should demonstrate compliance with information security requirements.

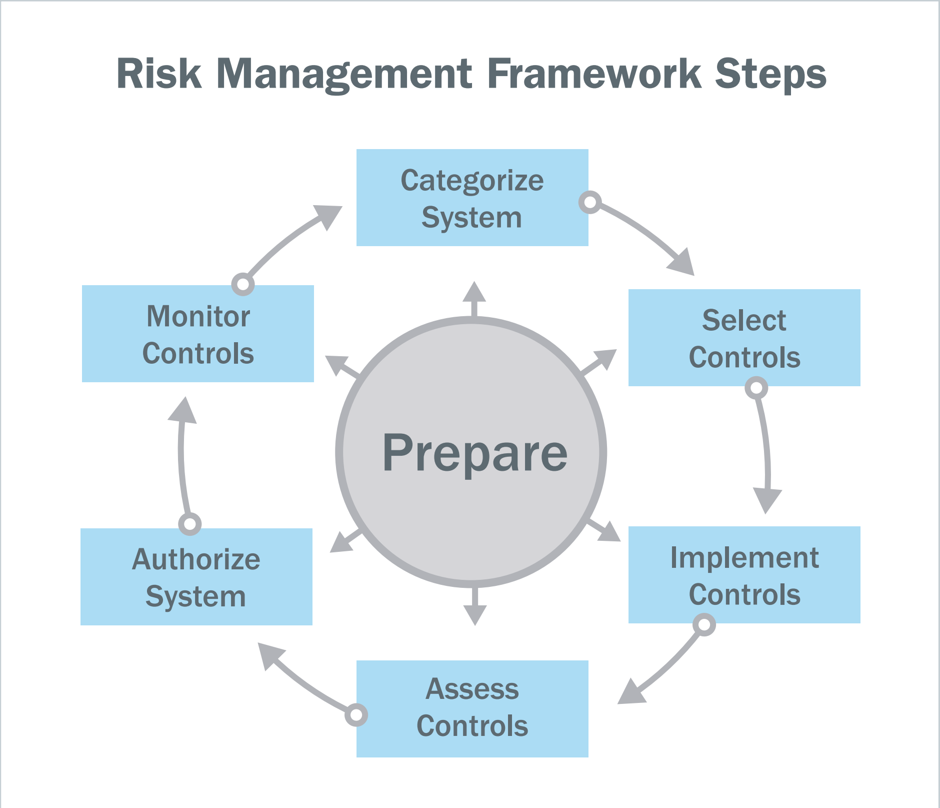

Figure 2. Managing cybersecurity risks using NIST's RMF. *Image by Anuj Sanghvi and Fred Zietz, NREL*

Risk Management Framework

As directed by FISMA, the National Institute of Standards and Technology (NIST) created the Risk Management Framework (RMF) to help organizations assess and manage risks to their information and systems. The RMF is a six-step process to guide individuals responsible for mission processes in the development of an enterprise cybersecurity program. It uses NIST Special Publication 800-53 for an extensive list of controls relevant to securing federal information systems, which are organized by related families.[3] The RMF provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations. Further detail is provided in NIST Special Publication 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* and associated publications.

Executive Orders on Cybersecurity

Executive Order 14028, Improving the Nation's Cybersecurity, signed May 12, 2021, requires federal agencies to enhance cybersecurity and software supply chain integrity. The federal government must develop mechanisms for information sharing, implement plans for zero-trust architecture, identify security gaps in the supply chain, form a safety board, initialize playbooks for incident response, and improve cybersecurity mitigation strategies and capabilities.

Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, signed May 11, 2017, requires all federal owners and operators of critical infrastructure to use NIST's Framework for Improving Critical Infrastructure Cybersecurity, commonly referred to as the Cybersecurity Framework (CSF), to manage cybersecurity risk. The executive order recognizes the increasing interconnectedness of federal information and operational systems and requires agency heads to ensure appropriate risk management for the agency's enterprise and for the Executive Branch as a whole.

Per Executive Order 13800, federal agencies are required to use the CSF, or any successor document, to manage the agency's cybersecurity risk to critical systems, including AMI. Additionally, it holds agency heads accountable by the president for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes. Results of the evaluation can be incorporated into the agency's EMIS planning process by reference. Further detail is provided in the NIST white paper, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1."

Federal Risk and Authorization Management Program

Software as a Service (SaaS), where software applications are hosted in a cloud-based environment and associated with a license, is becoming increasingly more common in the space of EMIS and beyond. The Federal Risk and Authorization Management Program (FedRAMP)[4] provides standardized low, medium, and high classifications that

[3] National Institute of Standards and Technology. 2020. *Security and Privacy Controls for Federal Information Systems and Organizations.* Washington, D.C.: U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5.

[4] Learn more about understanding baselines and impact levels in FedRAMP: https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

certify systems that use SaaS based on their security implications and potential impact. These classification levels are based on three security objectives:

- **Confidentiality**—Information access and disclosure includes means for protecting personal privacy and proprietary information.
- **Integrity**—Stored information is sufficiently guarded against modification or destruction.
- **Availability**—Access to information is timely and reliable.[5]

Systems categorized in the "low" classification have fewer controls associated with them, and typically lower cost and a quicker approval process, whereas the "high" classification has the opposite effect. When a cloud system is being used, the Office of Management and Budget requires that agencies use the FedRAMP requirements when completing the RMF.

FEMP Cybersecurity Tools and Resources

The Federal Energy Management Program (FEMP) supports tools and resources that help federal agencies assess their security posture, address potential vulnerabilities, and achieve EMIS cybersecurity compliance and authority to operate. As part of the EMIS planning process, agencies should include a description of how federal cybersecurity frameworks will be applied to secure the EMIS.

Facilities Cybersecurity Framework

The Facilities Cybersecurity Framework (FCF) is a publicly available web application that provides a self-assessment module optimized around cybersecurity needs for facility-related control systems. Adapted from the CSF, the FCF provides a common taxonomy and mechanism to help building stakeholders describe their current security posture, set a target state for cybersecurity, identify and prioritize opportunities for improvement, assess progress toward a target state, and communicate cybersecurity risk among stakeholders.[6]

Distributed Energy Resources Cybersecurity Framework

In 2019, the National Renewable Energy Laboratory (NREL) developed the Distributed Energy Resources Cybersecurity Framework (DER-CF) and accompanying web application to address the lack of guidance for securing distributed energy resources (DERs).[7] The web-based tool assists a federal facility's management team by bringing guidance and structure to the extensive array of cybersecurity controls applicable to DERs and walking the user through a three-pillar assessment framework. The DER-CF utilizes existing work encapsulated in the U.S. Department of Energy's Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) into a pillar focused on cybersecurity risk management, called Cybersecurity Governance.[8] To extend that content, NREL has developed two additional pillars—technical management and physical security—that focus on controls related to system-level settings and site security as it relates to DERs. Upon completion of an assessment, users are provided with a set of results that identify and assess their cyber and physical assets, as well as a customized, prioritized list of action items to help address potential vulnerabilities.

Distributed Energy Resources Risk Manager

NREL has also developed the Distributed Energy Resources Risk Manager (DER-RM) as an extended scope to the DER-CF. It specifically focuses on NIST's RMF process and guides users to develop appropriate reports required for achieving authority to operate.

The DER-RM was designed to be a standalone, downloadable application that is functional without external connections for the purpose of securely navigating through system-level questions. The DER-RM is a framework that generates documentation for the authorizing officer's review and includes an easy-to-interpret and customized report that identifies common vulnerabilities and prioritizes mitigation strategies.

Learn More About EMIS

Read more about cybersecurity planning for EMIS in FEMP's *Energy Management Information Systems Technical Resources Report:* energy.gov/eere/femp/articles/energy-management-information-systems-technical-resources-report.

For questions about EMIS, email Jason Koman at Jason.Koman@ee.doe.gov and Jefferey Murrell at Jefferey.Murrell@ee.doe.gov. ■

U.S. DEPARTMENT OF
ENERGY
Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

FEMP
Federal Energy Management Program

For more information, visit:
energy.gov/eere/femp

DOE/GO-102022-5680 · June 2022

[5] U.S. General Services Administration. 2017. "Understanding Baselines and Impact Levels in FedRAMP." Accessed June 26, 2020. https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

[6] Pacific Northwest National Laboratory. 2020. "Facility Cybersecurity Framework." Accessed June 26, 2020. https://facilitycyber.labworks.org/.

[7] Powell, Charisa, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds. 2019. *Guide to the Distributed Energy Resources Cybersecurity Framework*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75044. https://www.nrel.gov/docs/fy20osti/75044.pdf.

[8] U.S. Department of Energy. 2014. *Electric Subsector Cybersecurity Capability Maturity Model (ES- C2M2).* Washington, D.C. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.