FEMP
Federal Energy Management Program

Cybersecurity Considerations and Research Pathways for Grid-Interactive Efficient Buildings

Federal facilities serve critical missions and functions that require safe, reliable, and efficient operations. Digitization of several facility operations has increased the cost-effectiveness of energy usage and optimization of energy system performance. As the building controls landscape shifts to become more connected and smarter, building operators now face unique opportunities and challenges to adopt smart-enabled devices that can lower energy usage while also optimizing building system performance.

The grid-interactive efficient buildings (GEB) initiative aims to make buildings cleaner and more flexible through smart devices. Smart-enabled devices allow greater connectivity and control through remote operations and provide crucial data for analytics and increased efficiency. GEBs enable demand flexibility that has the potential to reduce electrical costs and transform the grid edge where buildings connect to power grids. This operation of interconnected systems, if not designed with cybersecurity practices, causes security gaps and introduces potential attack paths by adversarial and non-adversarial entities leading to disruption of operations.

GEB and Dependencies

Smart technologies such as on-site distributed energy systems, advanced metering infrastructure, and other Internet-of-Things devices serving advanced data analytics to management systems enable demand response services while providing energy savings. For effective GEB operations, it is important to realize, document, and manage risks of dependent systems that provide interconnectivity and critical data exchange pathways. These dependent systems and operations vary from power monitoring sensors and applications; lighting controls; heating, ventilation, and air conditioning controls; building automation system controls; safety sensors; first responder links; and other systems that eventually roll up and enable utility interconnection.

Illustration from Getty Images, 1424196888.

Cybersecurity Considerations

Cybersecurity pillars include data confidentiality, integrity, and availability (CIA) and are the basis of assessing risks to mission function based on impacts to the CIA triad. It is also the basis of how agencies perform Risk Management Framework (RMF) duties by selecting and assessing National Institute of Standards and Technology (NIST) security controls to achieve and maintain Authorization to Operate. For GEB technologies that support building decarbonization, understanding the CIA impacts of all system functions is critical.

On-site distributed energy resources (DERs), including bidirectional electric vehicles, have complex system boundaries and require additional assessments during technology specification, procurement, and deployment stages to accurately identify, document, and mitigate cybersecurity risks.

GEB technologies can have physical impacts that are critical to outline and may vary based on the function and mission of the system. These potential physical impacts include:

- Human safety
- Business operations
- Tenant operations
- Third-party operations
- Wireless access
- System damage or failure
- Leakage of personally identifiable information (PII)
- Loss of financial data.

Smart buildings often rely on legacy communication protocols such as BACnet, which are inherently insecure. Several attack vectors can manipulate critical set points, thresholds, and control algorithms and require a holistic assessment approach to enable safe and reliable GEB operations.

Compliance Requirements

Under Federal Information Security and Modernization Act (FISMA) directives, federal agencies are required to follow NIST SP 800-37R2 RMF and NIST SP 800-53 for an extensive list of controls. GEB technologies are required to adhere to NIST Cybersecurity Framework functions—govern, identify, detect, protect, respond, and recover—to articulate system functions, capabilities, and operations while having appropriate measures in place. Several of these requirements have a list of diverse stakeholders who are responsible for incorporating cybersecurity compliance requirements; for example, a GEB technology manufacturer will be required to add several security functionalities to protect federal agency data and infrastructure and consequently follow the Federal Risk and Authorization Management (FedRAMP) certification and authorization process to deploy cloud technologies at federal agencies. Some of these products have a Software as a Service model, where applications are hosted in a cloud-based environment.

Other stakeholders such as GEB system owners, operators, and contractors have their own share of cybersecurity risks that need to be managed through the RMF process.

Cybersecurity Tools

The **Distributed Energy Resources Cybersecurity Framework (DER-CF)**[1] provides federal facility energy and building managers with a starting point to conduct fundamental cybersecurity governance, technical management, and physical security assessments. The DER-CF produces a prioritized action-item list and guidance on implementation and continuous improvements.

The **Distributed Energy Resource Risk Manager (DER-RM)**[2] is a user-friendly tool that helps navigate and implement one of the most widely trusted frameworks for information security, the NIST Risk Management Framework. It also enables streamlined management of Authorization to Operate documentation.

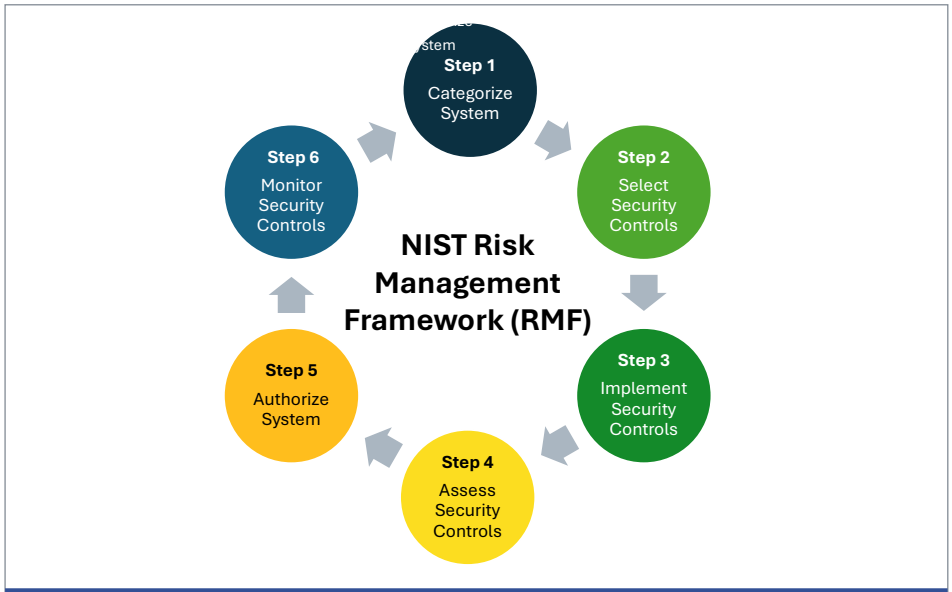

Figure 2. Building operators or managers must follow the six-step NIST RMF process when adopting GEB-related technology for their building(s). *Illustration from NREL.*

Learn More

Learn more about the following FEMP programs and initiatives.

Grid-Interactive Efficient Buildings: energy.gov/femp/grid-interactive-efficient-buildings-federal-agencies

Energy and Cybersecurity Integration: energy.gov/femp/energy-and-cybersecurity-integration. ■

References

Balamurugan, Sivasathya, Steve Granda, Selam Haile, Anya Petersen, Jing Wang, and Jiazhen Ling. 2024. *A Cybersecurity Testbed for Smart Buildings*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-85639. https://www.nrel.gov/docs/fy24osti/85639.pdf.

Building Technologies Office. 2020. *Grid-interactive Efficient Buildings: Projects Summary*. Washington, DC: Department of Energy. DOE/EE-2136. https://www.energy.gov/sites/default/files/2020/09/f79/bto-geb-project-summary-093020.pdf.

FEMP. 2022. "Energy Management Information Systems Cybersecurity Best Practices." Washington, DC: Department of Energy. DOE/GO-102022-5680. https://www.energy.gov/femp/articles energy-management-information-systems-cybersecurity-best-practices.

FEMP Federal Energy Management Program

1 NREL. "Distributed Energy Resources Cybersecurity Framework." Accessed September 2024. https://dercf.nrel.gov.

2 Thomas, Dana-Marie, Anuj Sanghvi, MD Touhiduzzaman, Paul Wand, and Tami Reynolds. 2024. *Guide to the Distributed Energy Resources Risk Management Framework*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-81715. https://www.nrel.gov/docs/fy22osti/81715.pdf.

For more information, visit:
energy.gov/femp

DOE/GO-102024-6446 • October 2024