Your Role in Defending Facility Systems from Cyber Attacks

May 13, 2020

Proudly Sponsored By

ProFM CREDENTIAL

FEA

Today's Session

- Introductions
- What is the Facilities Role in Cybersecurity?
- What do I Need to Know About Cybersecurity?
- Cybersecurity FBPTA Competencies
- Training Resources
- Q&A

Introductions

Maureen Roskoski, CFM, SFP, ProFM, ISO 22301 Lead Auditor
Senior Professional | Facility Engineering Associates

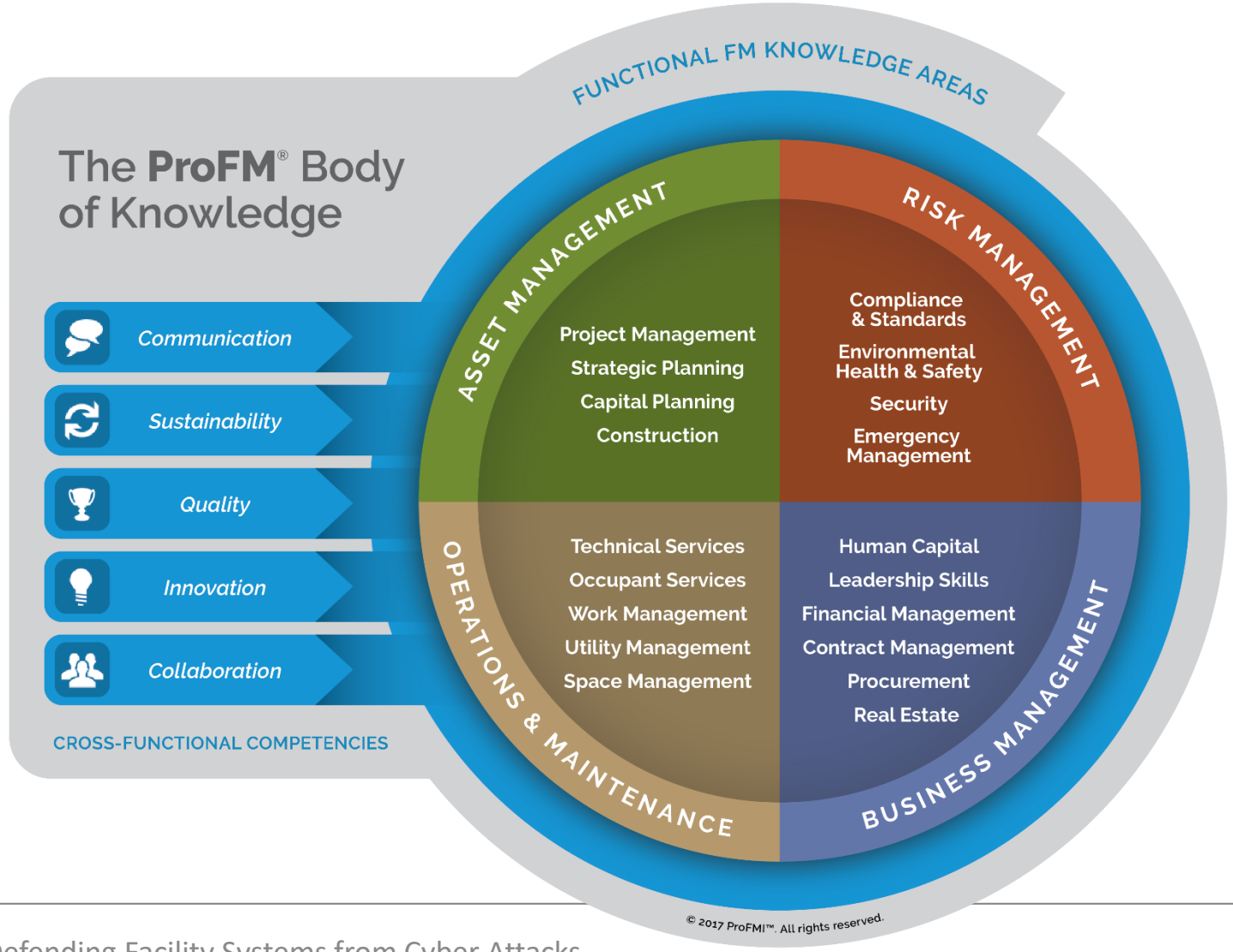
- 20+ years of experience in facility management, workforce development, sustainability, and resilience
- ProFM Instructor, BOC Instructor, IFMA SFP Instructor
- Leads FEA's contract with GSA for support of the Federal Buildings Personnel Training Act
- Developed competency model and career map for facilities and energy workforce – facilitescareermap.feapc.com

Today is World FM Day

- Thanks for all you do, every day!
- Visit www.ProFMi.org/world-fm-day-2020 to see messages of gratitude and appreciation from around the world
- You are #FMSuperHeroes to all of us!

ProFM Credential

- ProFM defines the **knowledge, skills, abilities,** and **behaviors** required for facility managers to be successful now and in the future.
- Based on study of 3300 professionals across 93 countries
- Key considerations:
  - U.S. Federal Buildings Personnel Training Act (FBPTA)
  - ISO 41000 Standards



WHAT IS THE FACILITIES ROLE IN CYBERSECURITY?

Information Technology (IT) vs. Operational Technology (OT) / Control Systems (CS)

KEY SYSTEM DIFFERENCES

DESIGN AND OPERATION

IT SYSTEMS EMPHASIZE

CONFIDENTIALITY

Enterprise information systems network
ERP, CRM, email, financial systems
Business-supporting applications
Mature environment / routine patching

OT / CS SYSTEMS EMPHASIZE

AVAILABILITY

Building management systems (BMS)
Energy control (lights and efficiency)
Environmental systems (HVAC)
Security (CCTV, access, fire suppression)
Ancillary systems (elevators, lighting)
PLC, SCADA, ICS, IIoT, HMI
The "forgotten network" / rare patches & updates

POORLY PATCHED
SYSTEMS

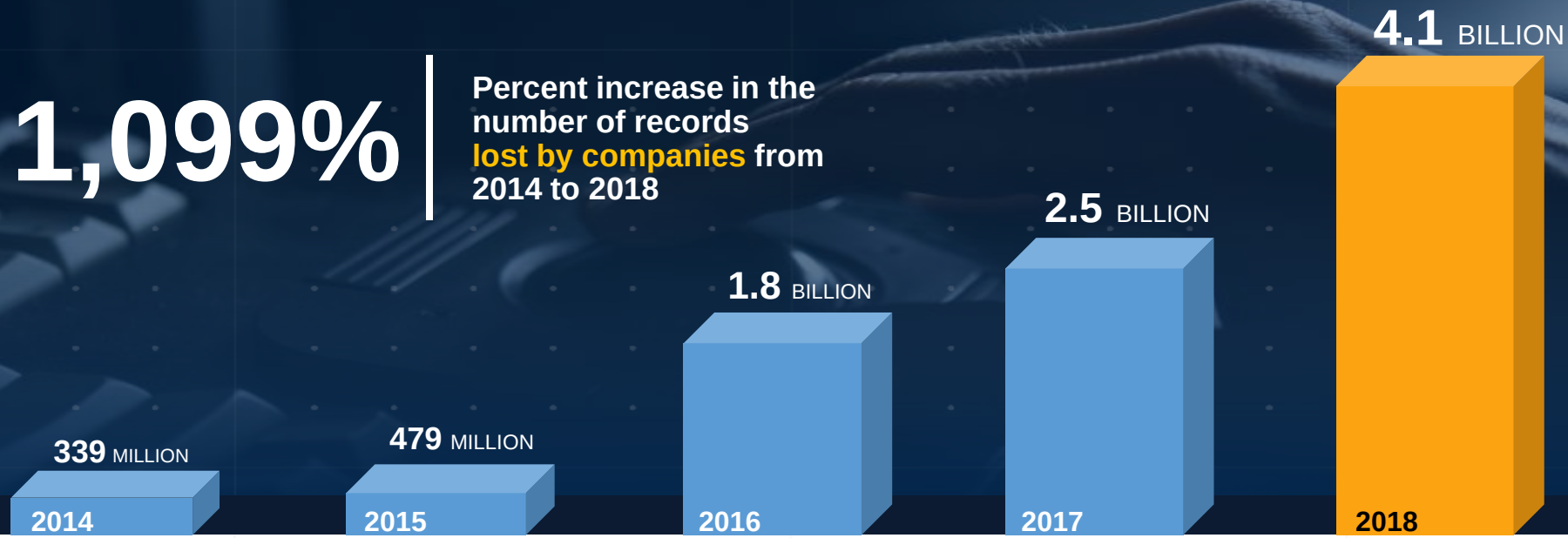
Allow adversaries to lurk undiscovered for **200+ Days**

UNCLASSIFIED

HACKS & BREACHES
ARE ON THE RISE

1,099%

Percent increase in the number of records lost by companies from 2014 to 2018



ebay • Anthem • YAHOO! • EQUIFAX • twitter

J.P.Morgan • ASHLEY MADISON.COM • myspace • UBER • Marriott

UNCLASSIFIED

KSAs: Knowledge

Facility Engineering

- Facility design, construction, and operations criteria and standards
- Capabilities and function of building systems, equipment controls and meters
- Procedures involved in troubleshooting, maintenance and repair of systems
- Laws, regulations, codes and policies regarding safe and secure operations of facilities
- Capital planning and continuity of operations plans

Cybersecurity for OT

Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82)

UFC 4-010-06 Cybersecurity of Facility-Related Control Systems

Risk Management Framework

Industry related cyber threats and vulnerabilities

Secure configuration management techniques

Supply Chain Risk Management

Tactics, Techniques and Procedures

IT Professionals

- Computer networking concepts, design, protocols, and security
- Capabilities and applications of network equipment and devices
- Network and system diagnostics, tools, and testing
- Intrusion detection and continuous monitoring techniques
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy
- Business continuity and disaster recovery continuity of operations plans

Emphasis in Federal Workforce Skills Gap in Cybersecurity

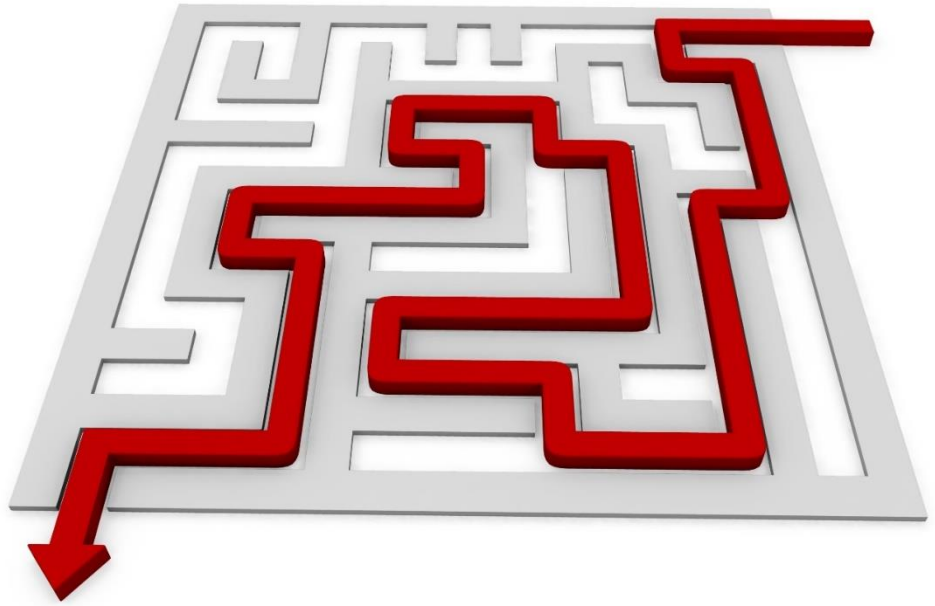
- Increased emphasis on critical importance of building and sustaining a world-class cyber workforce
  - National Cyber Strategy
  - President's Management Agenda
  - Executive Order 13800
  - Executive Order on America's Cybersecurity Workforce
- DoD is requesting information to assist the Government in identifying and evaluating skill and training gaps in Federal and non-Federal cybersecurity personnel
  - Critical Infrastructure Sectors
  - Defense Critical Infrastructure
  - DoD Platform Information Technologies (PIT)
- EO on America's Cybersecurity Workforce places particular emphasis on "cyber-physical systems (CPS) for which safety and reliability depend on secure control systems…"

Cybersecurity FBPTA Competencies Working Group

- **Why:** Clear vulnerability and gap in FBPTA Competency Model
- **What:**
  - Johns Hopkins study of gaps in current models, proposed fixes
  - GSA convened expert group to develop cyber competencies
  - Expert group reviewed, prioritized JH study's proposed fixes
  - GSA consolidated into 2019 Update
- **Who:** Experts from Facility IT Security at GSA, DoD, VA, SSA

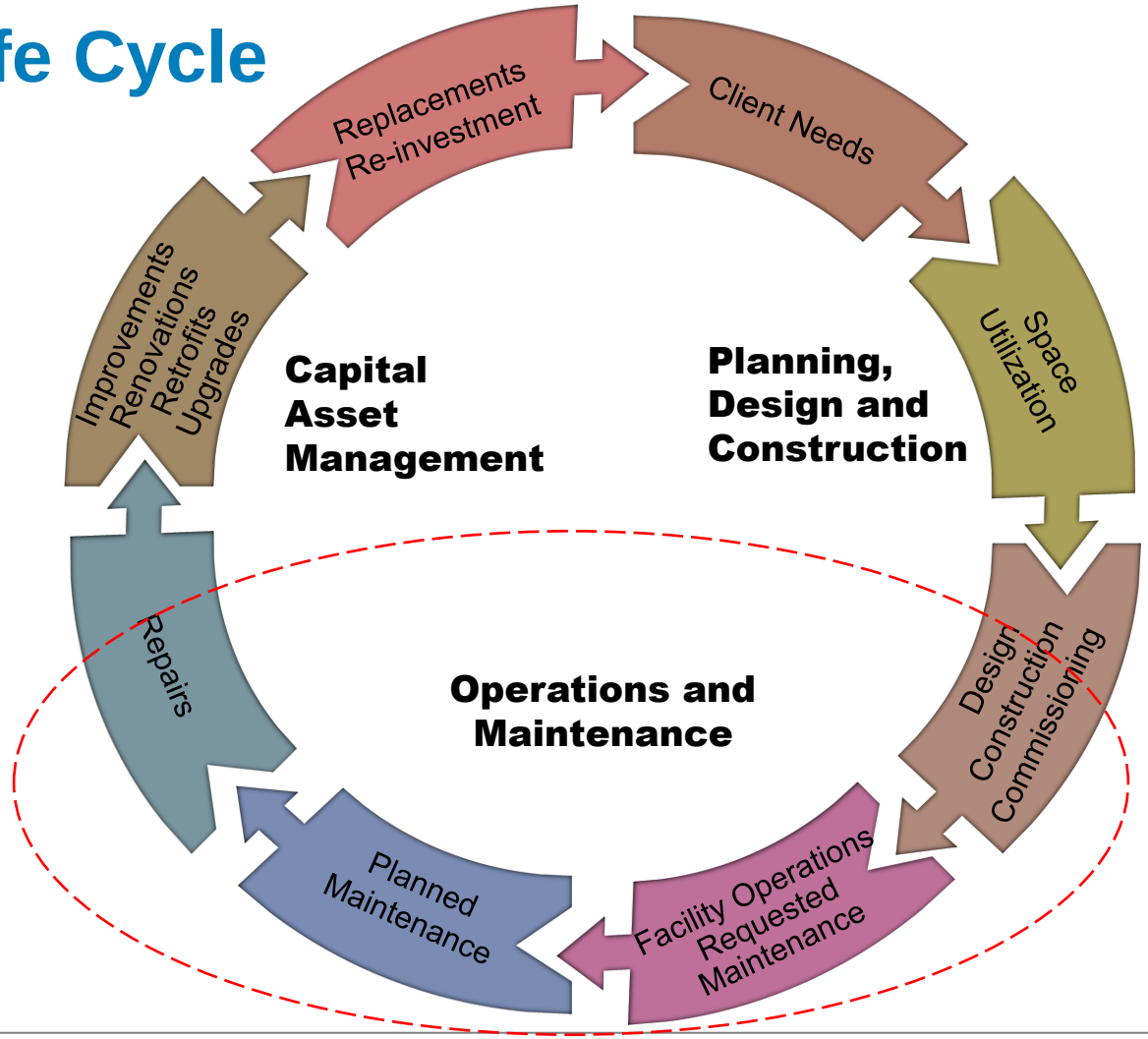
FBPTA – What does it require?

- Core Competencies for Federal buildings personnel
- Recommended Curriculum and Continuing Education
- Annual updates to Competencies and Curriculum
- Compliance by all Federal buildings personnel
- Method for contractor compliance



FBPTA – Who does it apply to?

Facility Life Cycle

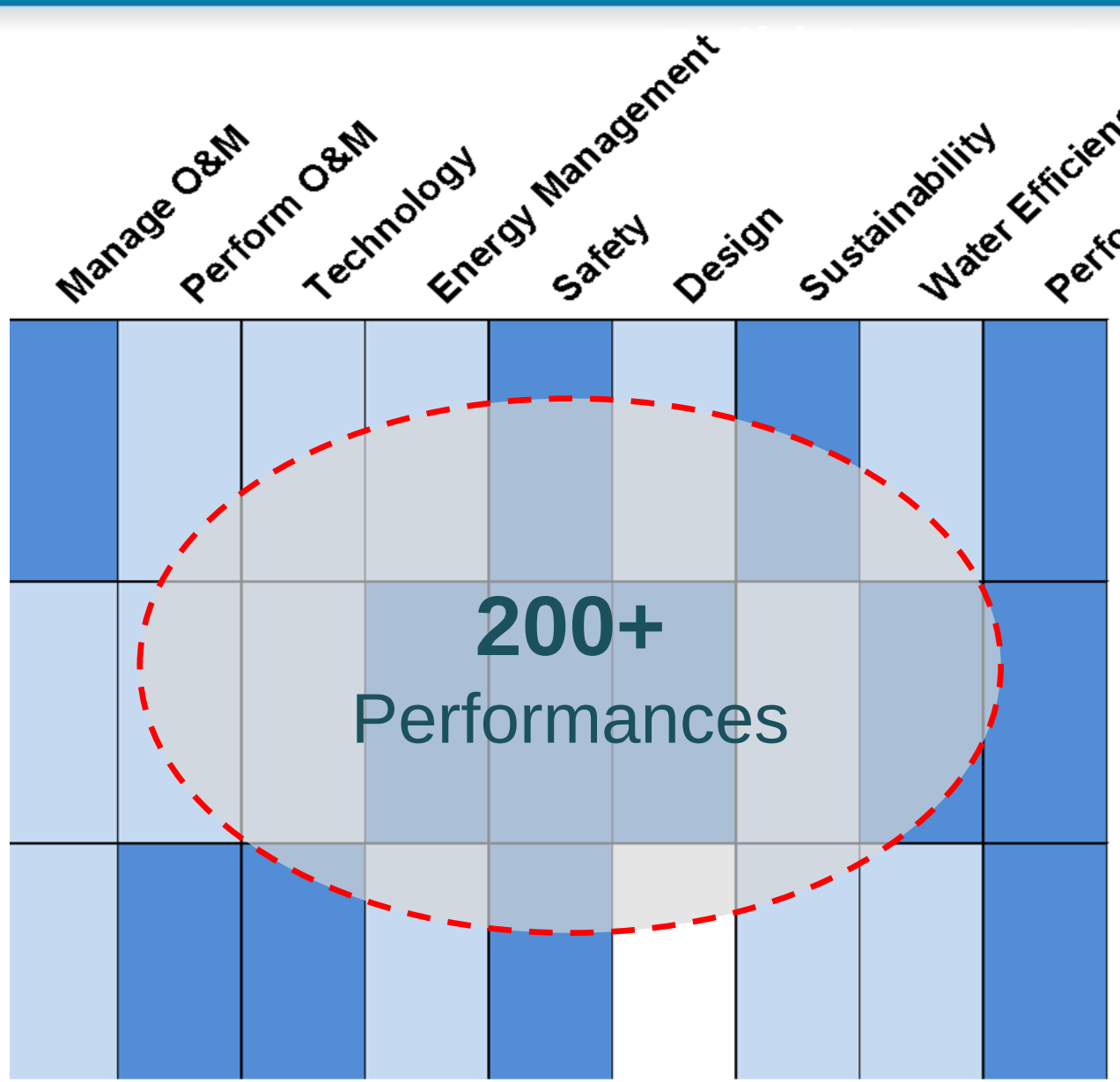


Facility Management

Energy Management

Building Operation

FBPTA Competency Model

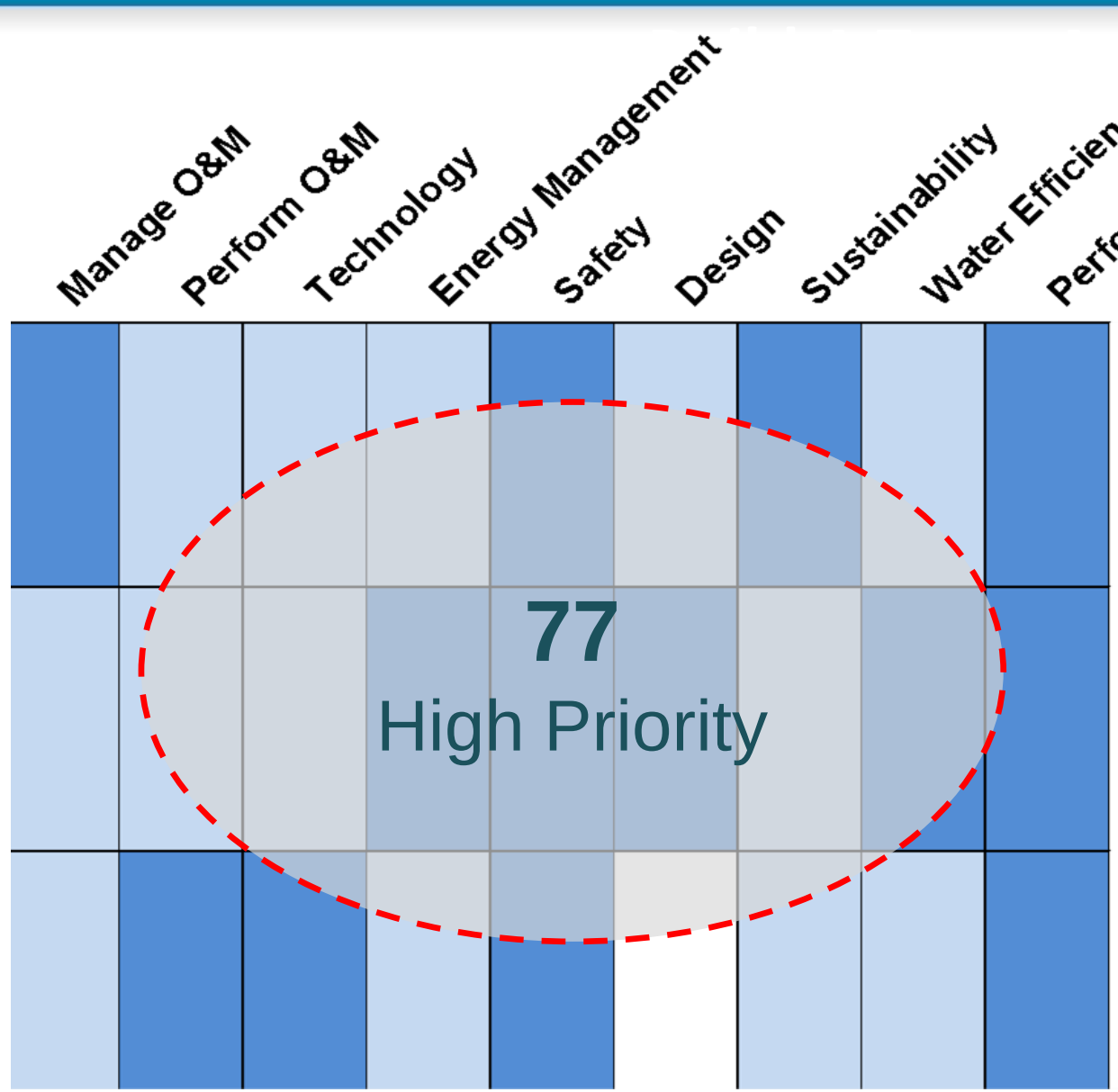


Facility Manager

Energy Manager

Building Operator

FBPTA Competency Model



Facility Manager

Energy Manager

Building Operator

Cyber security FBPTA competency framework

Competency Areas	Core Competencies	Performances	Performance Additional Comments
3. Technology	3.4 Cybersecurity in Facility Management and Building O&M	3.4.1. Demonstrate knowledge of cybersecurity requirements and configuration management of utility and building systems, subsystems, sensors, and other component devices to support continuity of operations.	Systems include: building automation systems, CMMS, Energy Management and Information systems, advanced meters, lighting systems, microgrids
		3.4.2 Demonstrate knowledge of how to conduct cybersecurity and risk assessments for building systems, including inventory of critical assets, and identify vulnerable systems.	Includes the magnitude of harm that could result from the unauthorized access, use, disclosure, disru information and information assets of the organization.
		3.4.3 Demonstrate knowledge of how to implement policies and procedures that are based on risk assessments.	Risk assessments identify how to cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information
		3.4.4 Demonstrate knowledge of how to develop subordinate plans to provide adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.	
		3.4.5. Demonstrate knowledge of how to identify and respond to cyber alerts, vulnerabilities, changes in system controls, and incident response regarding threats to the cybersecurity of systems, subsystems, sensors, and other component devices.	Includes application of proactive and reactive system patches/updates and ability to oversee implementation.
		3.4.6. Demonstrate knowledge of how to perform continuous monitoring of control systems and identify system instability.	
		3.4.7. Demonstrate knowledge of control systems' and recognizing abnormal behavior and anomalies.	
		3.4.8. Demonstrate knowledge of procedures for maintaining authority to operate (ATO) building systems.	Federal specific performance
		3.4.9. Demonstrate knowledge of communication procedures regarding alerts, vulnerabilities, and incident response including when (and to whom) to report abnormal operations.	Federal specific performance: Incidence response reporting is an agency specific requirement
		3.4.10. Demonstrate knowledge of cyber security technologies in accordance with relevant regulatory requirements, including hardware, software, and firmware.	
		3.4.11. Demonstrate knowledge of how to identify, address, and escalate issues where conflicting or competing policy, standards, and regulations create vulnerabilities in control systems.	
	3.5 Cybersecurity in Design and Acquisition	3.5.1. Demonstrate knowledge and ability to incorporate cybersecurity requirements during requirements development and design of facilities and associated control systems.	
		3.5.2 Demonstrate knowledge of cybersecurity requirements that must be included in procurement specifications for new systems and upgrading/modification specifications for existing systems.	Identify and include technical requirements needed to procure systems, subsystems, sensors, and other component devices with appropriate cybersecurity controls and capabilities to ensure the mission of the asset(s). This applies also to long-term requirements of ESPCs and leases
		3.5.3. Demonstrate knowledge and ability to ensure cybersecurity requirements are appropriately addressed in contract procedures and requirements for long-term maintenance agreements.	ESPCs, ownership of utility generation and distribution for assets not owned or operated by the government
		3.5.4 Demonstrate ability to assess cyber commissioning technical requirements needed to ensure delivery, cyber security, and quality of services/products.	currently done by commissioning agents, training them in cyber security and checklists
		3.5.5. Demonstrate familiarity with incorporating cybersecurity requirements into lease language and occupancy agreements for systems, subsystems, sensors, and other component devices.	
		3.5.6. Demonstrate ability to identify, address, and escalate issues where new emerging technologies and cybersecurity requirements affect costs and budgeting.	
		3.5.7. Demonstrate knowledge of how to ensure external vendors and contractors follow cyber hygiene requirements	Related to procurement (DFARS 7012 regulations) and FAR reference
		3.5.8. Demonstrate ability to recognize and understand the role of cyber security requirements in the ecosystem of integrated project delivery.	

3.4.2 Demonstrate knowledge of how to conduct cybersecurity and risk assessments for building systems, including inventory of critical assets, and identify vulnerable systems.

- *Includes the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.* (FM, EM)

Cyber security FBPTA competency framework

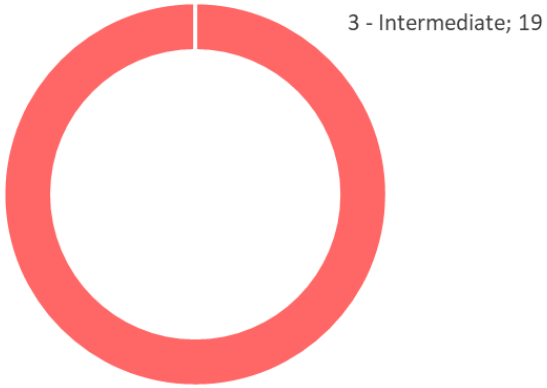
Competency Areas	Core Competencies	Performances	Performance Additional Comments
3. Technology	3.4 Cybersecurity in Facility Management and Building O&M	3.4.1. Demonstrate knowledge of cybersecurity requirements and configuration management of utility and building systems, subsystems, sensors, and other component devices to support continuity of operations.	Systems include: building automation systems, CMMS, Energy Management and Information systems, advanced meters, lighting systems, microgrids
		3.4.2 Demonstrate knowledge of how to conduct cybersecurity and risk assessments for building systems, including inventory of critical assets, and identify vulnerable systems.	Includes the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.
		3.4.3 Demonstrate knowledge of how to implement policies and procedures that are based on risk assessments.	Risk assessments identify how to cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information
		3.4.4 Demonstrate knowledge of how to develop subordinate plans to provide adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.	
		3.4.5. Demonstrate knowledge of how to identify and respond to cyber alerts, vulnerabilities, changes in system controls, and incident response regarding threats to the cybersecurity of systems, subsystems, sensors, and other component devices.	Includes application of proactive and reactive system patches/updates and ability to oversee implementation.
		3.4.6. Demonstrate knowledge of how to perform continuous monitoring of control systems and identify system instability.	
		3.4.7. Demonstrate knowledge of control systems' and recognizing abnormal behavior and anomalies.	
		3.4.8. Demonstrate knowledge of procedures for maintaining authority to operate (ATO) building systems.	Federal specific performance
		3.4.9. Demonstrate knowledge of communication procedures regarding alerts, vulnerabilities, and incident response including when (and to whom) to report abnormal operations.	Federal specific performance: Incidence response reporting is an agency specific requirement
		3.4.10. Demonstrate knowledge of cyber security technologies in accordance with relevant regulatory requirements, including hardware, software, and firmware.	
		3.4.11. Demonstrate knowledge of how to identify, address, and escalate issues where conflicting or competing policy, standards, and regulations create vulnerabilities in control systems.	
	3.5 Cybersecurity in Design and Acquisition	3.5.1. Demonstrate knowledge and ability to incorporate cybersecurity requirements during requirements development and design of facilities and associated control systems.	
		3.5.2 Demonstrate knowledge of cybersecurity requirements that must be included in procurement specifications for new systems and upgrading/modification specifications for existing systems.	Identify and include technical requirements needed to procure systems, subsystems, sensors, and other component devices with appropriate cybersecurity controls and capabilities to ensure the mission of the asset(s). This applies also to long-term requirements of ESPCs and leases
		3.5.3. Demonstrate knowledge and ability to ensure cybersecurity requirements are appropriately addressed in contract procedures and requirements for long-term maintenance agreements.	ESPCs, ownership of utility generation and distribution for assets not owned or operated by the government
		3.5.4 Demonstrate ability to assess cyber commissioning technical requirements needed to ensure delivery, cyber security, and quality of services/products.	currently done by commissioning agents, training them in cyber security and checklists
		3.5.5. Demonstrate familiarity with incorporating cybersecurity requirements into lease language and occupancy agreements for systems, subsystems, sensors, and other component devices.	
		3.5.6. Demonstrate ability to identify, address, and escalate issues where new emerging technologies and cybersecurity requirements affect costs and budgeting.	
		3.5.7. Demonstrate knowledge of how to ensure external vendors and contractors follow cyber hygiene requirements	Related to procurement (DFARS 7012 regulations) and FAR reference
		3.5.8. Demonstrate ability to recognize and understand the role of cyber security requirements in the ecosystem of integrated project delivery.	

3.5.5. Demonstrate familiarity with incorporating cybersecurity requirements into lease language and occupancy agreements for systems, subsystems, sensors, and other component devices.

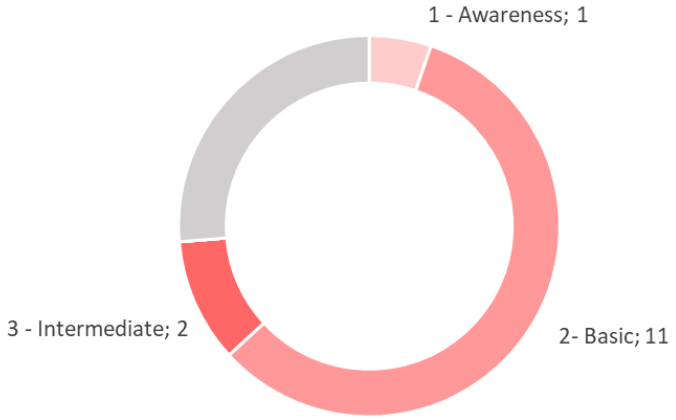
(FM, EM)

Position Profiles – Cyber Security Competencies Proficiency Levels

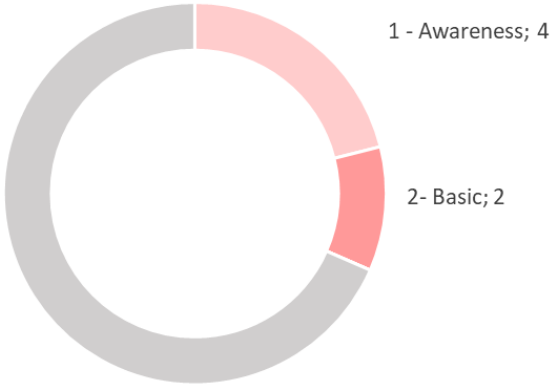
Energy Manager (EM)



Facility Manager (FM)



Facility Operator (FO)



KEY

Level 1: Awareness – Applies the competency in the simplest situations. Requires close and extensive guidance.

Level 2: Basic - Applies the competency in somewhat difficult situations. Requires frequent guidance.

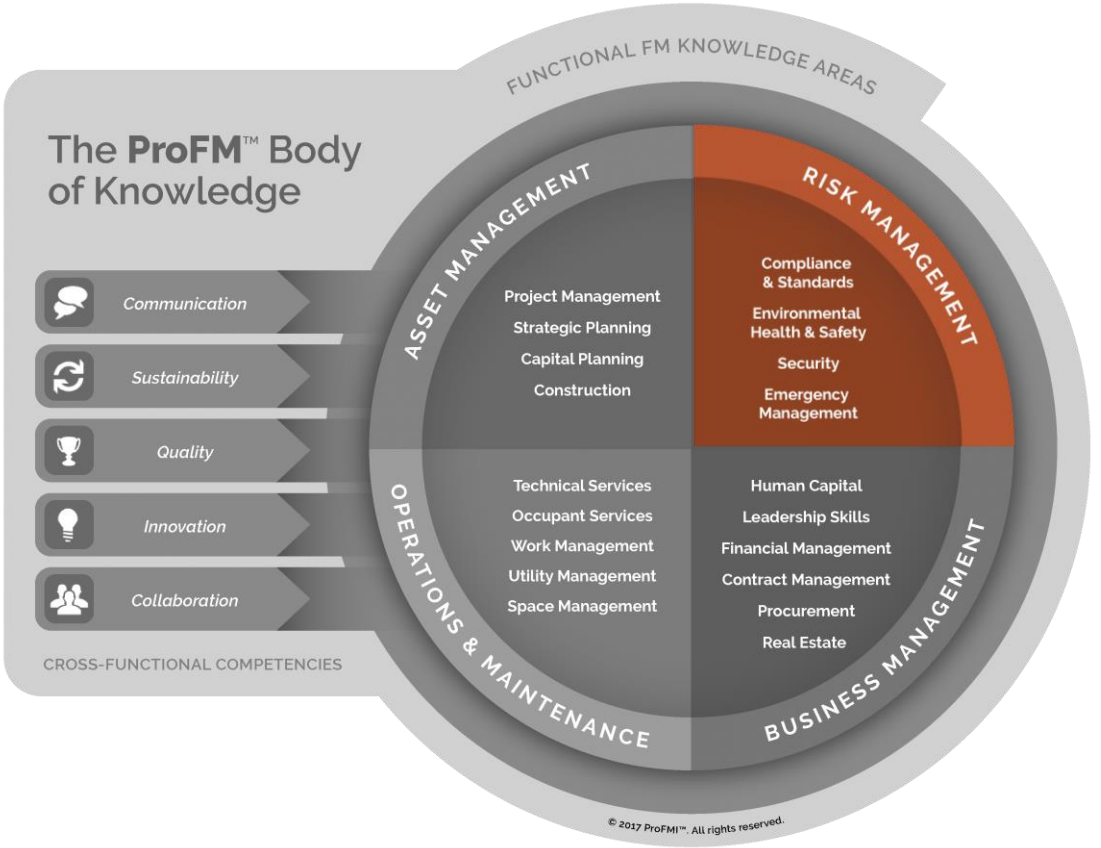
Level 3: Intermediate – Applies the competency in difficult situations. Requires occasional guidance.

Level 4: Advanced - Applies the competency in considerably difficult situations. Generally, requires little or no guidance.

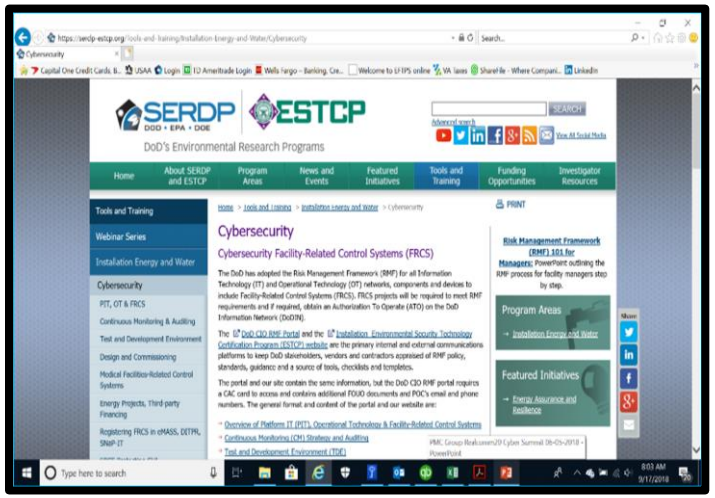
Level 5: Expert - Applies the competency in exceptionally difficult situations. Serves as a key resource and advises others.

Cybersecurity in ProFM

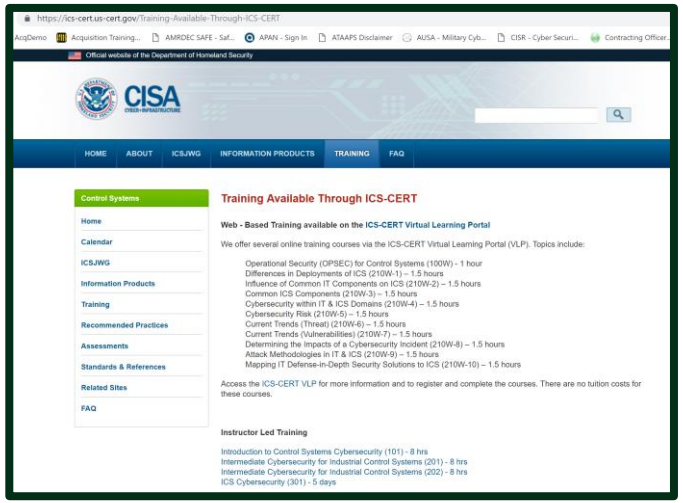
- 3 levels of cyber risk
- Confidentiality, Integrity, Availability (CIA) base standards
- Sources of risk
- Types of cyber attackers
- Vulnerabilities
- Managing cybersecurity risks
- Cybersecurity checklist



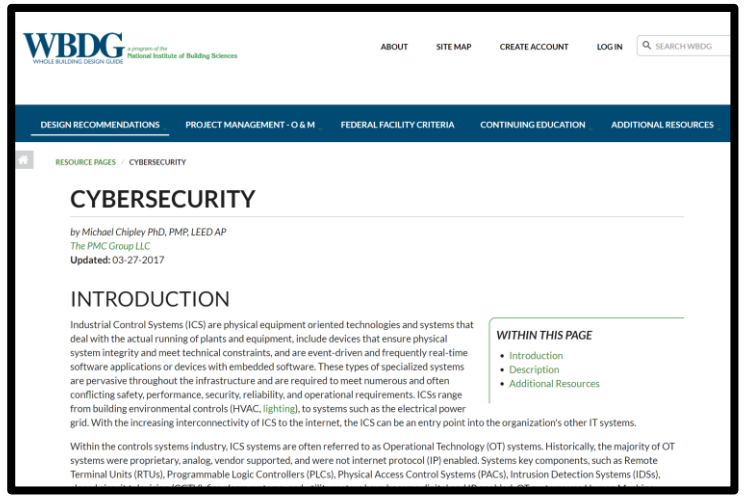
Other Training Resources



https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity

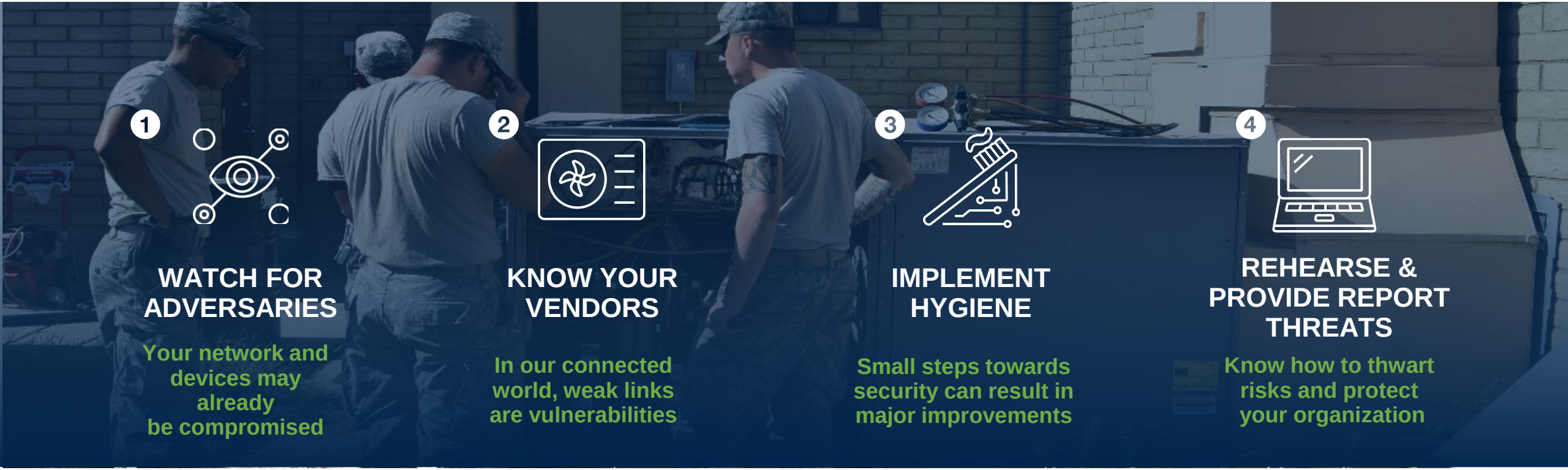


https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT



http://www.wbdg.org/resources/cybersecurity

Key Focus Areas For Any Manager



1

WATCH FOR ADVERSARIES

Your network and devices may already be compromised

2

KNOW YOUR VENDORS

In our connected world, weak links are vulnerabilities

3

IMPLEMENT HYGIENE

Small steps towards security can result in major improvements

4

REHEARSE & PROVIDE REPORT THREATS

Know how to thwart risks and protect your organization

It is critical to be proactive and take the necessary measures to ensure the security of your devices and systems. Strong defense begins with YOU.

FBPTA Resources

Resource	Website
Facilities Management Institute – Houses Accelerate FM, contains FBPTA information, and other workforce resources	https://sftool.gov/assess
Accelerate FM – Professional development planning and FBPTA compliance documentation tool	https://afm.fmi.gov
FEDSAT – Skills assessment tool to assess competency related to high priority FBPTA performances	www.sftool.gov/fedsat
Building Retuning - Set of courses and resources on tuning buildings developed by PNNL	http://retuningtraining.labworks.org/training/lms/
Career Map Tool – Career mapping tool that shows entry points and career progression within energy and facilities industry	https://facilitiescareermap.feapc.com

Questions?

Cyber Security

Maureen Roskoski
Facility Engineering Associates
maureen.roskoski@feapc.com
feapc.com

ProFM Credential

Randy Olson
ProFMI
randyo@profmi.org
www.ProFMi.org

Three ProFM Scholarships Available – Apply by June 1

Build on your career experience and elevate your FM knowledge and skills. This scholarship is for FM professionals with at least 5 years of experience in the industry.

Prepare yourself for a career in FM. This scholarship is for students enrolled in any level of post-secondary education, and those who have completed a program in the last 24 months.

Apply the skills and experience you gained through military service to your career in FM. This scholarship is available to veterans of the United States Military.

Scholarship recipients receive a fully-funded ProFM Credential Program, including study materials and final assessments.

Get details and apply online at www.ProFMi.org/scholarships