Pacific Northwest
NATIONAL LABORATORY

PNNL-30291

Facility Cybersecurity Framework Best Practices

August 2020

1 Sri Nikhil Gupta Gourisetti
2 Hayden Reeve
3 Julia A Rotondo
4 Grant T Richards

U.S. DEPARTMENT OF ENERGY | Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-30291

Facility Cybersecurity Framework Best Practices

August 2020

1 Sri Nikhil Gupta Gourisetti
2 Hayden Reeve
3 Julia A Rotondo
4 Grant T Richards

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Acronyms and Abbreviations

A/V	Audio/Visual
BAS	Building Automation System
C2M2	DOE Cybersecurity Capability Maturity Model
CCA	Critical Cyber Assets
CMT	Configuration Management Tools
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DoD	Department of Defense
DDoS	Distributed Denial-of-service
DOE	U.S. Department of Energy
EO	Executive Order
FBI	Federal Bureau of Investigations
FCF	Facilities Cybersecurity Framework
FEMP	Federal Energy Management Program
FISMA	Federal Information Security Management Act
HIPDS	Host Intrusion Detection and Prevention System
HNAP	Home Network Administration Protocol
IDPS	Intrusion Detection and Prevention System
IBMS	Intelligent Building Management Systems
ICS	Industrial Control System
ISP	Internet Service Provider
IT	Information technology
LAN	Local Area Network
MEEDS	Mitigation of External-exposure of Energy Delivery Systems
NBAD	Network Behavior Anomaly Detection
NIDPS	Network Intrusion Detection and Prevention System
NIST	National Institute of Standards and Technology
OT	Operational technology
PNNL	Pacific Northwest National Laboratory
RMF	Risk Management Framework
SIEM	Security Information and Event Management
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UPnP	Universal Plug and Play
VPN	Virtual Private Network
WPA/WPA2	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

Contents

Figures

Tables

1.0 Introduction

Federal facilities are increasingly adopting automation and connecting to the Internet creating an energy-internet-of-things environment that converges operational technology (OT) and information technology (IT). Today's buildings increasingly weave together networked sensors and cyber and physical systems that enable data to be collected, aggregated, exchanged, stored and monetized in new ways. Building technological advances have created new energy technology, services, markets and value creation opportunities (e.g. transactive energy, two-way grid communications, machine learning, and increased use of renewable and distributed energy resources). But as larger data sets are being exchanged at faster speeds between an increasing number of OT systems, it becomes more difficult to protect the security of the data lifecycle and the physical equipment it interacts with. These challenges are especially difficult to overcome because the economic and environmental gain (interoperability, big data, social networks and ubiquitous information sharing) are driving these prominent trends in the digital age. Often cybersecurity is an afterthought.

As the National Academies observed, connected building control systems "provide critical services that allow a building to meet the functional and operational needs of building occupants, but they can also be easy targets for hackers and people with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities; be used as an entry point to the traditional informational technology (IT) systems and data; cause physical destruction of building equipment (OT systems); and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event…. As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks."[1] Connectivity offers a tremendous opportunity for realizing our nation's energy efficiency and renewable energy goals, but at the cost of increased cyber risk to our buildings. Cyber threats and vulnerabilities, or even the perception of the increased risk they present, could hinder the adoption of smart, connected technology in buildings. For example, converting an electric grid into a smart grid incorporates smart metering and load management which leads to high risk of user and corporate privacy breach. Making systems easily accessible and available to anyone may motivate an attack on the power grid. While increasing cybersecurity awareness and risk management is essential, technology and resources available for facilities managers to deploy for protection vary widely.

The U.S. Department of Energy's (DOE) Federal Energy Management Program (FEMP) funded the Pacific Northwest National Laboratory (PNNL) to develop various cybersecurity tools, trainings, and reports to aid federal facility managers – and other building owners and operators – in better applying frameworks and lessons learned from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), risk management framework (RMF), DOE's cybersecurity capability maturity model (C2M2), and a wide variety of industry best practices and guidance documents (i.e., NIST 800 series, Department of Defense United Facilities Criteria). This set of tools, collectively known as the FEMP Facility-Related Control System Cyber Toolkit (FRCS Cyber Toolkit)[2], is focused on cybersecurity concerns from facility-related control systems and other operational technology (OT), such as industrial control systems (ICS). The FRCS Cyber Toolkit can be applied across six of the sixteen critical infrastructure sectors designated by the Department of Homeland Security, including government facilities, healthcare and public health,

[1] National Academies. March 2015. "Federal Facilities Council: Cybersecurity Building Control Systems." Accessed April 2020: https://www.nationalacademies.org/event/03-24-2015/federal-facilities-council-cybersecurity-building-control-systems

[2] https://facilitycyber.labworks.org/

commercial facilities (e.g., public assembly, offices, lodging), financial services (e.g., banking and insurance), emergency services (e.g., fire and police stations), and information technology. With increasingly converged IT and OT systems, it is crucial to address OT cybersecurity considerations and assess how the seam of these two systems could impact the overall cybersecurity posture of a facility.

Federal facilities have extensive federal- and agency-specific guidance on IT cybersecurity, though many of these policies and plans have minimal emphasis on connected OT devices, systems, or equipment. This can also apply across state and local facilities or the commercial building sector. In several cases, agencies organizations use ad hoc approaches such as tailoring their IT policy to address their OT cybersecurity policy resulting in security approaches that may not be scalable in or across facilities. Therefore, this report provides cybersecurity best practices to federal facility owners and operators to secure critical OT (and intersecting IT). Understanding and implementing the best practices contained within this report can be combined with the results of assessments conducted using the tools contained within the FRCS Cyber Toolkit, specifically the Facility Cybersecurity Framework (FCF) core assessment and checklist or the FCF Close-Loop Mapping Tool which builds best practices into the results, to provide additional insight into common vulnerabilities, threats, and potential impacts from cyberattacks.

The national opportunity and challenge to secure federal facilities such as smart buildings from emerging cyber threats cannot be overstated. Several documented findings from government reports indicate the growing threat of physical and cyber-based attacks on critical infrastructure systems. Securing federal facilities from emerging cyber threats is a process, not an end state, nor can a one-size-fits-all approach be taken. Enhancing the cybersecurity posture of facilities requires incorporating cybersecurity best policies, practices, and procedures. Facilities will continue to have unique cyber risks—different threats, vulnerabilities, and risk tolerances. Resources and tools within the FRCS Cyber Toolkit can help users determine how to assess their current posture, determine which activities are most important for critical service direction, prioritize investments to maximize security, and implement best practices.

The objective of this report is to provide an overview of the best possible method to use FRCS Cyber Toolkit (section 2.0) and distilled cybersecurity best practices for the federal facilities to address growing non-linear cyber threats (section 3.0). Recommendations in this document are aggregated from several NIST and other documents (see Appendix A for additional details).

2.0 FRCS Cyber Toolkit

Buildings are increasingly digitized and connected to cyberspace, enabling new opportunities to increase interoperability, connectivity, and energy efficiency, and to use renewable energy. Achieving continued energy reductions and reduce waste requires the secure development, deployment, and management of advanced building technology that is increasingly connected to the Internet and through the internet of things IoT and vulnerable to emerging cyber threats. Federal facilities must actively identify, prioritize, and mitigate the risks of cyber or physical attacks on facility-related control systems while maintaining the required level of service for efficient operations.

There are a variety of cybersecurity frameworks and policy drivers, including

- Federal Information Security Management Act (FISMA)
  - Resulted in the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- Executive Order (EO) 13800 Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- E.O. 13636 Improving Critical Infrastructure Cybersecurity
  - Resulted in the NIST Cybersecurity Framework (CSF)

Table 1. Cyber Framework Comparison

	NIST Cybersecurity Framework (CSF)	***Cybersecurity Maturity Model (C2M2)***	***NIST Risk Management Framework (RMF)***	***Cybersecurity Maturity Model Certification (CMMC)***
FEMP Available Tools	FCF & DERCF tools	F-C2M2 & DERCF tools	FCF-RMF tool	
Origin	NSIT SP 800-53	DOE- Office of Electricity	NIST SP 800-37	Department of Defense (DoD)
Required by	EO-13636 and 13800	Administration request	FISMA	DoD
Use Case	Assessment to comply with EO. Voluntary use by industry	Electric and oil and natural gas, State Department, others	Compliance with FISM. Codified by DoD in the UFC	Builds on DFARS
Stakeholder	Government, industry	DOE	Government (GSA, DoD)	DoD, defense industrial base
User	IT, OT, and facilities in government and industry	IT, OT, cyber experts	Team of cyber, facilities, IT	Team of cyber, facilities, IT procurement

To meet these policy drivers, PNNL's FRCS Cyber Toolkit includes resources to help federal facilities:

- Describe their current cybersecurity posture,

- Describe their target state for cybersecurity,
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process,
- Assess progress toward the target state,
- Communicate among internal and external stakeholders about cybersecurity risk

Assessments within the FRCS Cyber Toolkit complement, but does not replace, an organization's existing risk management process and cybersecurity program. Facility owners and operators can use their current processes and leverage FRCS Cyber Toolkit to identify opportunities to strengthen their cybersecurity risk management and adopt industry best practices. See Table 2 for a comparison of the tools and core resources within the FRCS Cyber Toolkit.

Table 2. FRCS Cyber Toolkit Comparison to Enhance Facility Cybersecurity

Tool	Description	When to Use
Facility Cybersecurity Framework (FCF)	Based on NIST CSF, helps users understand if they are compliant and discover cybersecurity gaps	If NIST CSF required (EO13800)
FCF Core Assessment	Technical assessment based on NIST CSF	To conduct cybersecurity assessment (describe current posture)
FCF-Risk Management Framework Assessment (FCF-RMF Hybrid)	Hybrid tool that maps RMF to FCF, recognizing that federal facilities may have different agency requirements.	If RMF required and also meet the requirement of E.O. 13800 CSF assessment
Qualitative Risk Assessment (QRA) or Risk registry	Inventory and manage CCAs, then qualitatively rank and group based on impact, vulnerability, and risk	Identify groups and potential risk of CCA
FCF Primer: Checklist Assessment (FCF-Primer)	FCF-Primer can be used to track cybersecurity gap mitigation process after conducting the core assessment. The FCF-Primer Checklist Assessment offers a simplified cybersecurity assessment (e.g. "yes" or "no" responses), which can aid sites just starting out or needing a less detailed assessment results (non-critical facilities or non-critical legacy OT with minimal connected OT).	Smaller number of CCAs, faster assessment
Comparative Evaluation	Users can compare multiple FCF Core Assessments or FCF-Primer Assessments to see how cybersecurity posture has changed between assessment or over the years	Compare cyber posture over time. Manage progress
FCF Training Game	Dynamic training game based on real-world OT-based cyber-attack scenarios that help users understand FCF.	Workforce development

Facilities Cybersecurity Capability Maturity Model (F-C2M2)	Based on DOE's Cybersecurity Capability Maturity Model, measure the sophistication or capabilities of a cybersecurity program	Develop and valuate cyber program capabilities
Management Priorities Tool (MPT)	Designed to capture high-level management cybersecurity and organizational goals and then compare against FRCS Cyber Toolkit assessment results to identify the technological gaps likely to raise to the management level.	Identifying the "key" cybersecurity gaps from management perspective communicate needs and track progress.
Automatic Policy Tool (AutoPol)	A tool that semi-automates cybersecurity policy review	Complete an assessment faster using previously identified existing plans and policies
Close-loop Mapping Tool	Uses outcomes of FRCS Cyber Toolkit assessments to shortlist potential threats that take advantage of gaps. Identifies best practices to mitigate	Targeted best practices to address cybersecurity gaps
Mitigation of Exposed Cyber FRCS	Uses existing MEEDS software to discover publicly exposed OT systems, their vulnerabilities, and assign risk scores. Once identified the tool can be used to visualize the OT network to perform safe active/passive scans.	OT enumeration followed by safe scanning
ArcGen	Provides illustrative OT architectures based on Purdue reference model. This can be used to conceptualize OT networks and for planning purposes	Secure OT network planning
		Access via: https://facilitycyber.labworks.org/

2.1 Facility Cybersecurity Framework Overview

This document provides an overview of best practices of each NIST CSF function which can be assessed and reviewed via the tools contained within the FRCS Cyber Toolkit. Of heightened value to assess cybersecurity posture are two specific Facility Cybersecurity Framework tools: the FCF Core Assessment tool and the FCF-Primer.

2.1.1 FCF Core Assessment Tool

The FCF core assessment tool is based on the NIST CSF and therefore provides five concurrent and continuous functions to Identify, Protect, Detect, Respond, and Recover from cyber threats and vulnerabilities to facilities. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's cybersecurity risk management. The FCF provides an actionable approach that can be easily adopted by an operator to enhance the organization's cybersecurity posture. The essence is captured in a set of "how-to" instructions for operators to adopt, adapt, and apply to their respective organizations. FCF Core Functions are defined in Figure 3. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the functions can be performed concurrently and continuously to form an operational culture to address dynamic cybersecurity risks.

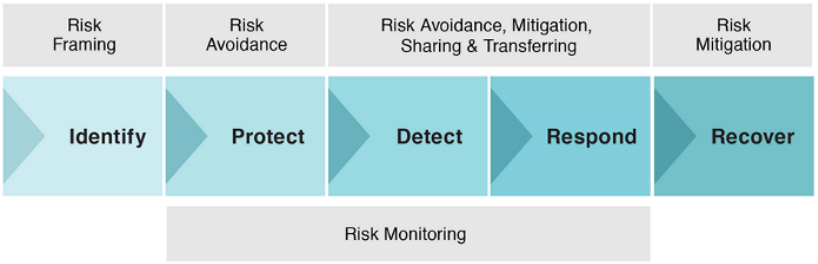

Figure 1. Outline of Facility Cybersecurity Framework

2.1.2 FCF Primer

The FCF-Primer[1] is meant to supplement, improve, and/or help facility owners enhance their cybersecurity posture. The FCF-Primer could be used by the facility owners to track their progress towards desired maturity. The FCF-Primer can be used before or after an assessment and it is a straightforward means of ensuring that the steps taken align with the organization's cybersecurity goals.

[1] https://facilitycyber.labworks.org/fcf_primer/about

3.0 Facility Cybersecurity Best Practices

The following sections provide a detailed description of each NIST CSF function, the key elements within that function, and example best practices for each element. These best practices are drawn from several sources including the NIST Manufacturing Profile[1], the Real Estate Cybersecurity Consortium (RECC)[2], and Building Owners and Managers Association (BOMA)[3]. The best practices are presented in escalating maturity levels (e.g. basic, intermediate, and advanced). The best practices should not be considered exhaustive and complete but are given as examples of efforts operators can take to increase their cybersecurity posture.

Table 3. Ten High-Level Best Practices

	Description
1	**Know Your Facility** Facilities evolve. Establish system baseline and control how and when it is changed based on asset and configuration management.
2	**Increase Awareness** Facilities operators and owners know and document what is plugged-in, what security controls are built into a system during development and throughout its' lifecycle: initiation, development, implementation, operations, maintenance, disposal.
3	**Tackle Weakness** Have a mature patch and vulnerability management program with safe scanning and penetration testing, trend and impact analysis, and remediation. Those methods are non-trivial for OT networks and the process is often very different as compared to standard IT systems. For example, penetration testing on legacy OT systems can do permanent damage and cause significant downstream impacts. Therefore, scanning methods should be assessed for compatibility with OT system components, used with care and based on necessity.
4	**Respect and Save Memories** Ransomware is one of the most alarming and expensive attacks to respond to and recover from. Therefore, protect all critical data such as audit logs, configuration logs by keeping up to date along with your knowledge about them; ensure their security by encrypting and securing them on no/minimal access media.
5	**Maintain Healthy Boundaries** Strengthen your protection mechanisms by adding access control to every network connected software and hardware asset including physical access to locations in the building.

[1] https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile
[2] http://re-cc.com/
[3] https://www.boma.org/

6	**Improve Destructive Relationships** In order to protect data (especially in buildings with a lot of exchange), ensure the existence of current detailed data destruction policy with identified authority controls to approve data destruction. *Questions to be asked: Dual authentication to proceed? Delete the back-ups?*
7	**Speak Your Mind** Communicate the effectiveness of current security plans and procedures. Learn from the existing process, identify needed updates and improvements and clearly and vigorously communicate to management.
8	**Get Personal** Incorporate good cybersecurity practices in actions such as screen assets (software, hardware, and personnel), de-provisioning systems such as access-accounts, hardware and software configurations.
9	**Move On** It is critical to keep plans related to Protection mechanisms, Incident Response, and Incident Recovery up to date in order to protect CCAs from similar cyberattacks in the future.
10	**Live to Learn to Live** Learn from incidents. Improve the protection policies, procedures, and control mechanisms. Strengthen the facility systems and components day-by-day.

3.1 Identify

The goal of the Identify Function is to identify cyber risks and vulnerabilities and to then develop the organizational capacity to manage cybersecurity risk to systems, assets, data, and capabilities. In other words, the objective is to identify and inventory critical cyber assets (CCAs) and develop the organizational capacity to manage cybersecurity risk to systems, assets, data and capabilities. Examples of CCAs are shown in Fig. 2 and are distinctively defined as Information Technology (IT) and Operational Technology (OT) that are connected to the operation of the organization and associated organizational goals. When identifying CCAs in the facility, it is important to clearly distinguish between two categories of facility assets:

- **Information Technology (IT)** - The application of computers to store, study, retrieve, transmit, and manipulate data, or information, often in the context of a business or other enterprise. IT is considered a subset of information and communications technology (ICT).
- **Operational Technology (OT)** - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.

To realize the goal of the Identify Function, various risk framing tools such as the risk registry tool (link: https://facilitycyber.labworks.org/fcf/qra) are facilitated through FCF. Activities in the Identify function help the facility operators focus and prioritize efforts, consistent with the organizations risk management strategy and business needs. The six key elements of this function are: *Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy and Supply Chain Risk Management*.

Figure 2. Illustration of Common Critical Cyber Asssets Found in Facilities

3.1.1 Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. Example best practices include:

- **Basic**: Document an inventory of the facility system components, firmware, software, system architecture, and external connections and services.
- **Intermediate**: Develop and maintain a technical target architecture and implement architectural review board to obtain alignment across IT and OT disciplines. Identify individuals who are both responsible and accountable for maintaining system inventory. Update the inventory as an integral part of component installations, removals, and system updates.
- **Advanced**: Employ automated mechanisms (where safe and feasible) to automatically update inventories and detect the presence of unauthorized software, hardware and firmware components within the system.

3.1.2 Business Environment

The organization's mission, objectives, stakeholders, activities and resulting security and resiliency requirements are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. Example best practices include:

- **Basic**: The impact of a cybersecurity compromise of facility systems on critical business functions is understood and assessed versus required levels of service.
- **Intermediate**: Define recovery time objectives and recovery point objectives for the resumption of essential facility processes. Perform a criticality analysis to assess facility functions against these requirements and prioritize systems and components needing improvement.
- **Advanced**: Determine resiliency and continuity plans for the loss of critical services to the facility (e.g. loss of power) or compromise (e.g. fire, malware) critical assets such as intelligent building management system (IBMS) workstations

3.1.3 Governance

The policies, procedures, and processes to manage and monitor the organization's regulatory and legal risk, environmental and operational requirements are understood and inform the management of cybersecurity risk. Example best practices include:

- **Basic:** Develop, implement, and maintain written OT specific policies that will ensure proper protections are in place for the OT environment. This reduces the effort required to manage traditional IT policy exceptions and violations.
- **Intermediate:** Ensure the security policy includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the facility systems. Review and update the security policy as determined necessary. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by the facility systems.
- **Advanced:** Ensure that legal and regulatory requirements affecting the facility operations regarding cybersecurity are understood and managed.

3.1.4 Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Example best practices include:

- **Basic**: Identify and track vulnerabilities of assets in inventory. Use manufacturer and other industry (ICS-CERT) vulnerability databases to assess inventory cyber vulnerability exposure. Furthermore, identify common threats and impacts to the network. Incorporate the data pertaining to emerging risks, threats, and vulnerabilities in the security planning process to facilitate a robust understanding of the likelihood and impact of cybersecurity events (at least at a qualitative/subjective level).
- **Intermediate**: Develop a plan for continuous monitoring of the security posture of the facility systems to facilitate ongoing awareness of vulnerabilities. Establish and maintain ongoing contact with security groups and associations and receive security alerts and

advisories. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross organization information-sharing capability. Collaborate and share information about potential vulnerabilities and incidents on a timely basis.

- **Advanced**: Provide contractual language to account for disclosure of potential vulnerabilities. Conduct performance/load testing and penetration testing on the facility with care to ensure that facility systems are not adversely impacted by the testing process. Identify where facility system vulnerabilities may be exposed to adversaries.

3.1.5 Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Example best practices include:

- **Basic**: Establish a risk management process for the facility that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally.
- **Intermediate**: Define the risk tolerance for the facility and ensure the risk tolerance is informed by the facility's role in the organization's overall risk analysis.

3.1.6 Supply Chain Risk Management

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks. Example best practices include:

- **Basic**: Develop, monitor and practice a controlled acquisition process for OT and OT systems. Controlled acquisition is a key element of managing inventory
- **Intermediate**: Provide contractual language for seller to notify buyer of any known security vulnerabilities for the duration of the contract. Breach Notification (specify time period), including physical breach, as well as loss of mobile media, and must cooperate with Owner (including notification duties if requested)
- **Advanced**: Provide contractual language to have OT provider (seller) produce certification of vulnerable-free devices. Require notifications be given by third party service contractors for any personnel transfers, termination, or transition involving personnel with physical or logical access to the OT system components.

3.2 Protect

The goal of the Protect Function is to protect assets by introducing facility operators to cyber protection techniques that enable risk control through risk avoidance (see more in Fig. 3). The Protect function will help operators develop and implement the appropriate safeguards to increase a facility's cybersecurity posture. It supports the ability to limit or contain the impact of a potential cybersecurity event. The six core elements of this function are: *Identify Management Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology*.

3.2.1 Identify Management and Access Control

Access to physical and logical assets and associated facilities is limited to authorize users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. Example best practices include:

- **Basic**: Establish and manage identification mechanisms and credentials for users and devices of the OT systems. Employ automated mechanisms where feasible to support the management and auditing of information system credentials. Disable or rename default user accounts. Many OT devices ship with default administrative or configuration user settings that should be disabled or renamed. Use only named accounts for a one-to-one, person-to-account credentials. Deploy physical security techniques. Ensure key IT/OT devices are physically secured with access controlled to those resources who have a need to know will prevent unauthorized access. Enforce the “least privilege” levels for IBMS users and maintenance personnel
- **Intermediate**: Deactivate system credentials after a specified time period of inactivity, unless this would result in a compromise to safe operation of the process. Monitor the OT system for atypical use of system credentials. Credentials associated with significant risk are disabled. System communication architectures leverage segmented networks, micro-segmentation and other cybersecurity techniques, such as:
  - Application whitelisting
  - Layered network architectures/VLANs
  - Firewalls, access control lists or unified threat management devices
- **Advanced**: Enforce micro-segmentation or zero trust networks. Use multi-tier firewall deployment architectures with demilitarized zones (DMZ) in needed locations (example: between the enterprise network and the OT network). Deploy advanced physical and cyber security techniques and intrusion detection/prevention systems (IDS/IPS) for continuous monitoring and real-time network protection detection.

3.2.2 Awareness and Training

The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements. Example best practices include:

- **Basic**: Ensure that users with privileged access to the facility systems understand the requirements and responsibilities of their assignments. Establish standards for measuring, building, and validating individual qualifications for privileged users.
- **Intermediate**: Establish and enforce security requirements for third-party providers and users. Ensure that third-party providers understand their responsibilities regarding the security of the OT systems and the responsibilities of their assignments. Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.
- **Advanced**: Incorporate insider threat recognition and reporting into security awareness training.

3.2.3 Data Security

Information and records (data) are managed consistently with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. Example best practices include:

- **Basic**: Devices use industry-standard protocols for encryption of data in transit and at rest. This includes associated system file and databases. Encrypting critical data will minimize compromise and use of your data assets.
- **Intermediate**: Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items.
- **Advanced**: Address end of life systems (including firmware, software and embedded modules) through a risk assessment. Ensure leadership both understands and responds to risks (remediate, avoid, transfer, accept, etc.)

3.2.4 Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. Example best practices include:

- **Basic**: Develop, document, and maintain a baseline configuration for the OT systems. Baseline configurations include for example, information about OT system components (e.g. software license information, software version numbers, HMI and other industrial control system (ICS) component applications, software, operating systems, current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.
- **Intermediate**: Employ configuration change control for the OT systems and its components. Conduct security impact analyses in connection with change control reviews. Test, validate, and document changes to the OT systems before implementing the changes on the operational system. Review and authorize proposed configuration-controlled changes prior to implementing them on the OT systems.
- **Advanced**: Verify the reliability and integrity of backups. Coordinate backup testing with organizational elements responsible for related plans. Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed. Include into contingency plan testing the conducting of restorations from backup data. Store critical OT systems backup information separately.

3.2.5 Maintenance

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. Example best practices include:

- **Basic**: Devices are patchable via properly authenticated mechanism. Security is an on-going process and IT/OT devices must be remediated/patched per corporate standards
- I**ntermediate**: Do you have a procedure to positively identify and log IBMS maintenance personnel prior to and during IBMS access?
- **Advanced**: Enforce approval requirements, control, and monitoring, of remote maintenance activities. Employ strong authenticators, record keeping, and session termination for remote maintenance.

3.2.6 Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements. Example best practices include:

- **Basic**: Can you identify and authenticate persons through events logs, etc., who have logical access to your IBMS? Configure devices and systems to perform minimum required services and duties for which they are intended for. Ensure the device configurations limit the use of services based on the functions required by the IoT device. Common example: Prevent email and internet access from device management consoles
- **Intermediate**: Disable defined functions, ports, protocols, and services within the system deemed to be unnecessary. Employ technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs. If capable, disable or configure to meet organization security standards: Bluetooth-Wireless-NTP-SMTP-FTP-Telnet-SSH-Remote Logging-Non-essential device services. Ensure the device configurations limit the use of services based on the functions required by the IoT device.
- **Advanced**: Do you have an appropriate level of protection for your IBMS enabled wireless connectivity? Control the flow of information within the system and between interconnected systems. Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network. Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers. Limit external connections to the system. Manage the interface for external telecommunication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted, reviewing and documenting each exception to the traffic flow policy.

Figure 3 (next page) outlines several key protection measures to defend a facility against cyberattacks.

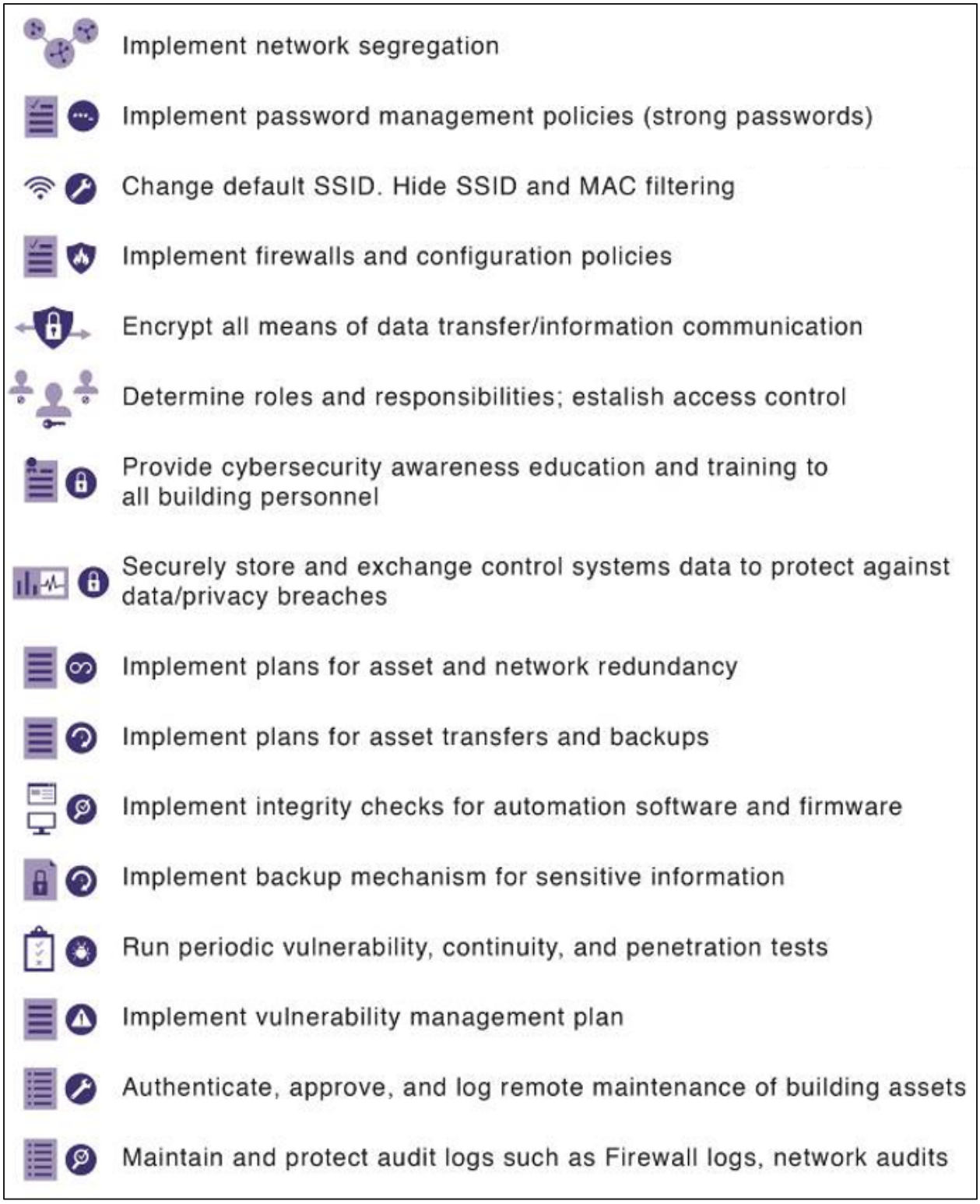

Figure 3. Key Protection Measures to Defend a Facility Against Cyberattacks

3.3 Detect

The goal of the Detect Function is to highlight techniques that enable the detection of malicious cyber activity. The Detect Function enables timely discovery of cybersecurity events. The three key elements of this function are: *Anomalies and Events, Security Continuous Monitoring, and Detection Processes*. This function defines the path towards concluding an anomaly as a cyberattack as depicted in Figure 4.

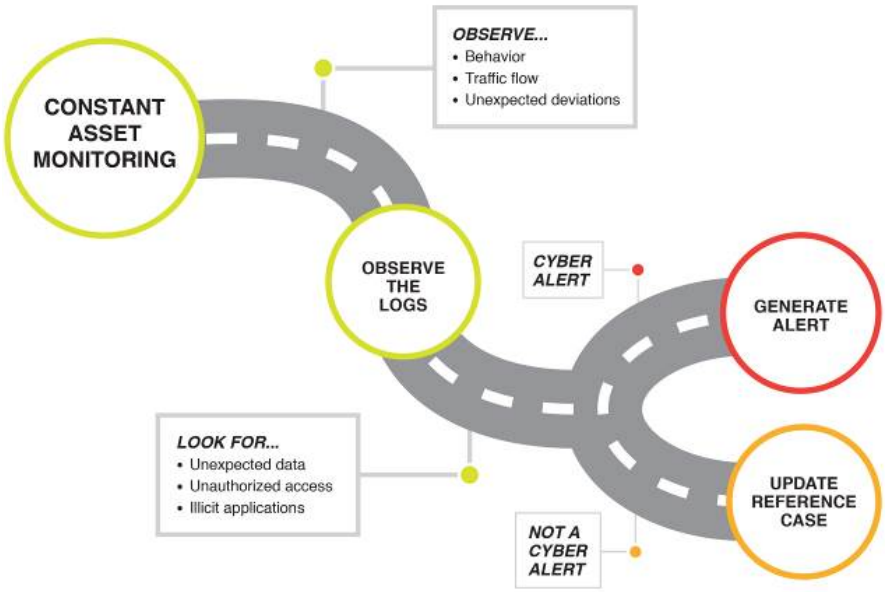

Figure 4. Detection Path Towards Concluding an Anomaly as a Cyberattack

The Detect Function also demonstrates the need for baseline operations for the critical assets and the means to use the reference cases to monitor for any deviations or unexpected behavior. Figure 5 shows an illustrative structure of a reference case that is also often referred to as baseline.

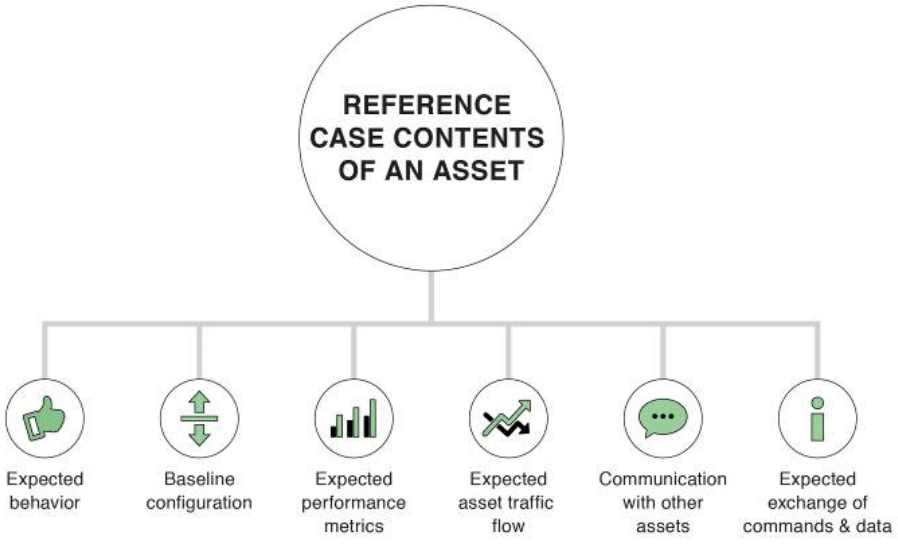

Figure 5. Illustrative Reference Case for Critical Cyber Assets

3.3.1 Anomalies & Events

Anomalous activity is detected in a timely manner. Potential impact of events is understood. Example best practices include:

- **Basic**: Ensure that a baseline of network operations and expected data flows for the system is developed, documented, and maintained to detect events.
- **Intermediate**: Review and analyze detected events within the OT system to determine negative impacts to operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.
- **Advanced**: Define incident alert thresholds and employ automated mechanisms where feasible to assist in the identification of security alert thresholds.

3.3.2 Security Continuous Monitoring

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Example best practices include:

- **Basic**: Conduct ongoing security status monitoring on the system for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies.
- **Intermediate**: Conduct ongoing security status monitoring of external service provider activity on the system. Detect attacks and indicators of potential attacks from external service providers. Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.
- **Advanced**: Conduct penetration testing and vulnerability scans on the system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process. Employ control system-specific vulnerability scanning tools and techniques where safe and feasible. Active vulnerability scanning, which introduces network traffic, is used with care on systems to ensure that system functions are not adversely impacted by the scanning process.

3.3.3 Detection Processes

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. Example best practices include:

- **Basic**: Define roles and responsibilities for detection activities on the system and ensure accountability.
- **Intermediate**: Communicate event detection information to defined personnel. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.
- **Advanced**: Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions. Ensure the security plan for the OT system provides for the review, testing, and continual improvement of the security detection processes. Employ independent teams to assess the detection process.

Conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the OT system.

3.4 Respond

The goal of this function is to respond to a cyberattack by developing and implementing the appropriate processes to effectively respond to a cybersecurity event. When both protection and detection techniques fail to prevent an attack, which can be expected to occur at times, it is critical for facility operators to know the best course of action to minimize impact. Key attributes of a cybersecurity response plan include, but not limited to:

1. Perform forensic analysis and preserve evidence and findings.
2. Isolate the infected assets or part of the network, as needed. Ensure the continuity of as many business processes as possible by replacing the infected assets with off-the-shelf/backup assets.
3. Backup all data and revert the firmware/software on the assets to previous known stable patch. Efforts should also be made to save an image of the infected version on an offline/off-network device for further analysis.
4. Accumulate all technical details pertaining to asset reintegration (example: configuration and connectivity information, third party documents/datasheets, etc.).
5. Use the above technical details in the process of establishing mission priorities as sequence of recovery and asset/network reintegration depends on mission priorities.
6. Ensure that the newly connected/integrated assets/patches do not get infected and all known vulnerabilities are mitigated before integration.
7. Define and follow a sequence of reconnection –
8. Identify mission commander priorities. Then identify dependencies and develop reintegration sequence.
9. Reintegrate clean assets. Ensure that the assets are infection-free. Integrate the subsystem and the network layers.
10. Finally, the recovery phase should monitor the reintegrated components to ensure all evidence of the cyber incident has been eliminated from the network.

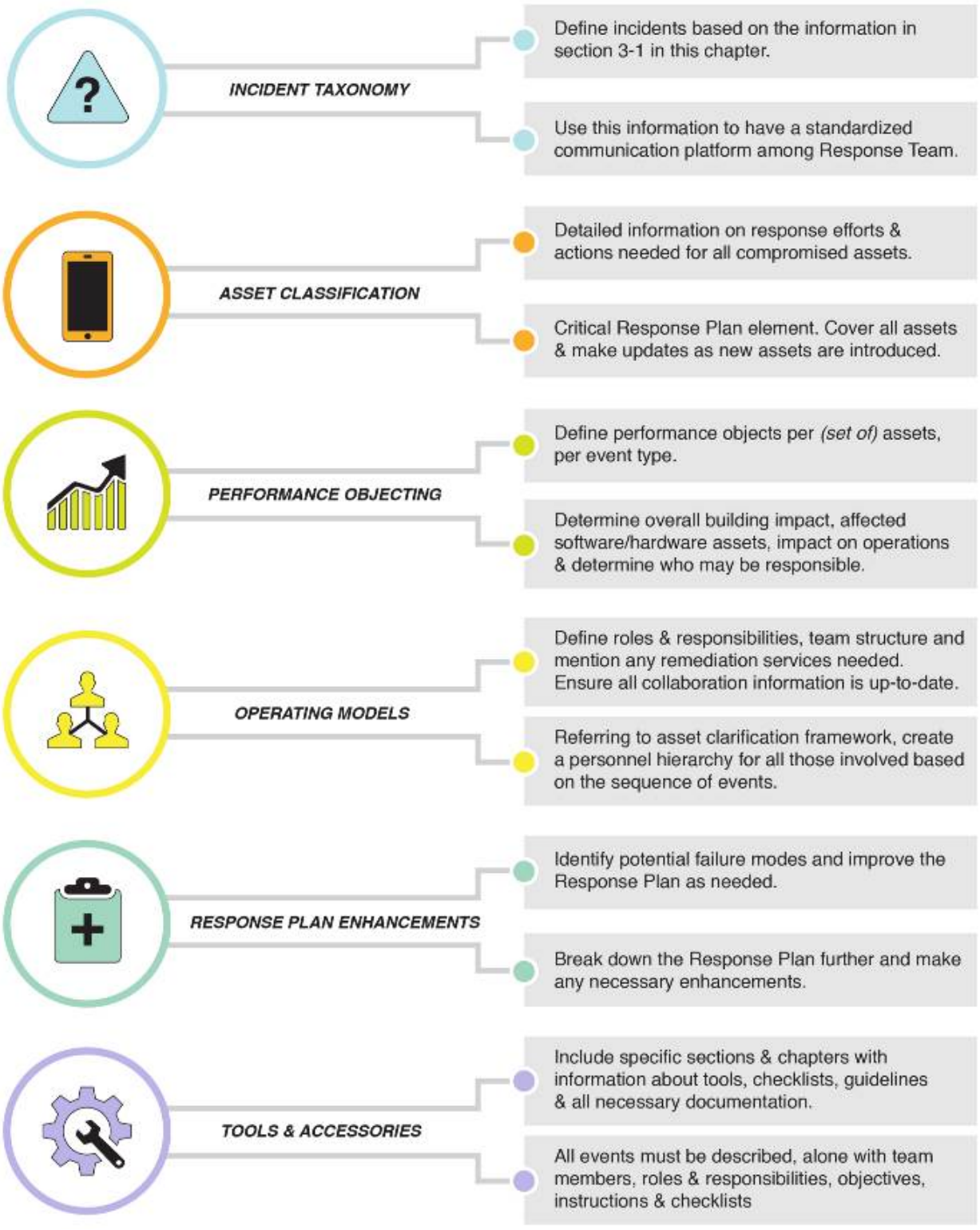

Figure 6. Critical Contents of a Cybersecurity Response Plan

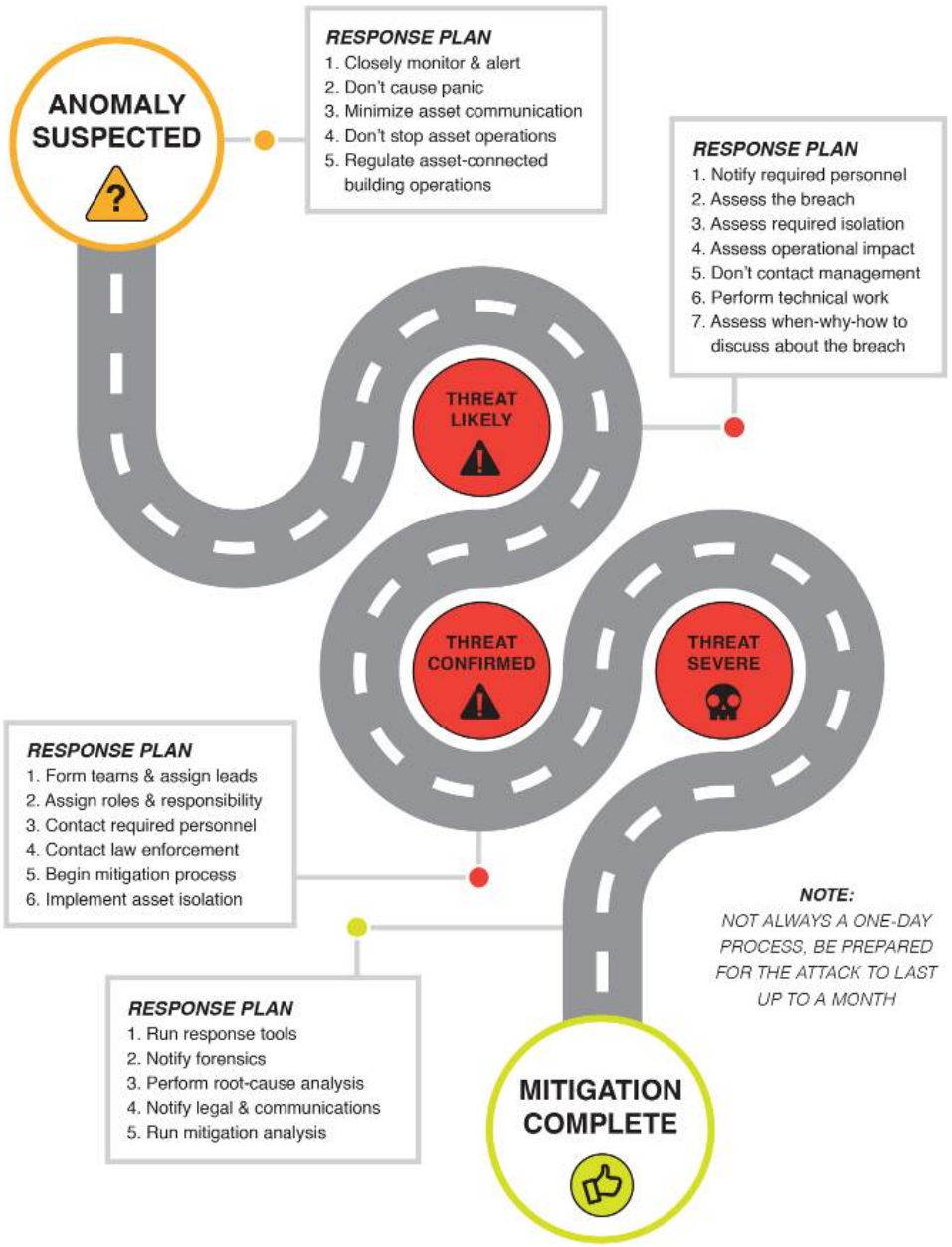

Figure 7. Implementation Path of a Response Plan Post-Cyber Intrusion Detection

The Respond function process provides facility operators with methodologies to respond to an incident. The five key elements of this function are: *Response Planning, Communication, Analysis, Mitigation, and Improvements*. Figure 6 depicts the contents of a response plan and Figure 7 depicts the implementation path of a response plan.

3.4.1 Response Planning

Response processes and procedures are executed and maintained, to ensure timely response to detect cybersecurity events. Example best practices include:

- **Basic**: Are your routine or non-routine incident response plans tested through desk-top exercises to a defined schedule?
- **Intermediate**: Do you have formal procedures for security breaches involving suspected unauthorized IBMS access?

3.4.2 Communication

Response activities are coordinated with internal and external stakeholders as appropriate to include external support from law enforcement agencies. Example best practices include:

- **Basic**: Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response. Employ prompt reporting to appropriate stakeholders for cybersecurity events on the OT system. Ensure that cybersecurity events on the OT system are reported consistent with the response plan.
- **Intermediate**: Employ automated mechanisms to assist in the reporting of cybersecurity events. Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example, mission/business owners, OT system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
- **Advanced**: Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness.

3.4.3 Analysis

Analysis is conducted to ensure adequate response and support recovery activities. Example best practices include:

- **Basic:** Perform investigation and forensics when a cybersecurity incident occurs.
- **Intermediate:** Perform incident impact analysis in an automated fashion and provide on-demand audit reviews, analysis and reporting. Categorize the incidents according to levels of severity and impacts.

3.4.4 Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. Example best practices include:

- **Basic**: Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
- **Intermediate**: Update the response plans to address changes to the organization, system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.

3.4.5 Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Example best practices include:

- **Basic**: Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

- **Intermediate**: Update the response plans to address changes to the organization, system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.

3.5 Recover

The goal of the Recover Function is to recover and return services to normal operation and reduce the impact of a cybersecurity event. The Recover Function provides insight on the creation and implementation of a recovery plan for facility operators. This plan will include solutions to recover compromised facilities assets, repair or replace damaged components, and return services to normal operation. The three key elements of this function are: *Recovery Planning, Improvements, and Communications*.

3.5.1 Recovery Planning

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. Example best practices include:

- **Basic**: Ensure that the contingency plans are up-to-date and execute documented procedures. Ensure that the backup systems are at the same level as the primary systems. Execute the recovery plan during or after a cybersecurity incident on the system. Restore the system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.
- **Intermediate**: Continue essential functions and services with little or no loss of operational continuity and sustain continuity until full system restoration.

3.5.2 Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities. Example best practices include:

- **Basic**: Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.
- **Intermediate**: Update the recovery plan to address changes to the organization, OT system, or environment of operation and problems encountered during plan implementation, execution, or testing. Ensure that updates are integrated into the recovery plans.

3.5.3 Communications

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Example best practices include:

- **Basic**: Ensure personnel understand recovery objectives and priorities, task sequences and assignment responsibilities for event recovery. Employ prompt reporting to appropriate stakeholders for cybersecurity events on the system. Ensure that cybersecurity events on the OT system are reported consistent with the recovery plan.
- **Intermediate**: Employ automated mechanisms to assist in the reporting of cybersecurity events. Coordinate cybersecurity recovery actions with all relevant stakeholders.
- **Advanced**: Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness.

4.0 Conclusion

This work describes key drivers for federal facilities to protect their OT from cyberattack by presenting an overview of available tools within the FRCS Cyber Toolkit and best practices, for any building owner or operator to better meet NIST CSF framework functions to identify, protect, detect, response and recover.

Appendix A – References

Building Owners and Managers Association. Cybersecurity." Building Owners and Managers Association International. Accessed November 2019. https://www.boma.org/BOMA/ResearchResources/Trends/Cybersecurity.aspx.

E.O. 13800, 82 FR 22391 (2017). "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Accessed June 2020: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

National Academies. March 2015. "Federal Facilities Council: Cybersecurity Building Control Systems." Accessed April 2020: https://www.nationalacademies.org/event/03-24-2015/federal-facilities-council-cybersecurity-building-control-systems

National Institute of Standards and Technology. March 2018. "Cybersecurity Framework Version 1.1." https://www.nist.gov/cyberframework/framework

National Institute of Standards and Technology. January 2015. "Security and Privacy Controls for Federal Information Systems and Organizations." *NIST 800-53 Rev 4*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

National Institute of Standards and Technology. September 2017. "Manufacturing Profile." https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile

Real Estate Cybersecurity Consortium. http://re-cc.com/

Reeve, Hayden et. al. March 2020. "Challenges and Opportunities to Secure Buildings from Cyber Threats." PNNL-29813. https://www.energy.gov/sites/prod/files/2020/05/f74/bto-pnnl-29813-securing-buildings-cyber-threats-051420.pdf

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov