An introduction to buildings cybersecurity framework

Conference Paper · November 2017

DOI: 10.1109/SSCI.2017.8285228

3 authors, including:

Sri Nikhil Gupta Gourisetti
Pacific Northwest National Laboratory
39 PUBLICATIONS **522** CITATIONS

SEE PROFILE

An Introduction to Buildings Cybersecurity Framework

Michael Mylrea, Sri Nikhil Gupta Gourisetti, *Member, IEEE*, Andrew Nicholls
Pacific Northwest National Laboratory
michael.mylrea@pnnl.gov, srinikhil.gourisetti@pnnl.gov, andrew.nicholls@pnnl.gov

***Abstract*—This paper presents an introduction to the Buildings Cybersecurity Framework (BCF). The BCF provides the organizations with a set of cybersecurity best practices, policies and procedures to improve their cybersecurity posture; defines structured methodologies to interact cybersecurity activities and outcomes from the executive to operations levels. The foundation of the BCF core is based on five core elements defined by the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover. Those five core elements were crafted to address evolving cybersecurity threats and vulnerabilities. With the BCF, an organization will be able to: assess their target cybersecurity state and current cybersecurity posture; identify and prioritize improvement opportunities and necessary actions by continuous and repeatable process; assess progress towards the target state; and communicate cybersecurity risk among internal and external stakeholders. This paper is a miniature of the ~100-page Buildings Cybersecurity Framework, and the goal of this paper is to explicate the applicability of BCF in different types of buildings such as Residential, Small Commercial, Large Commercial, and Federal buildings. Note that the framework itself is a detailed version of the various aspects discussed in this paper.**

Keywords—*Buildings; Cybersecurity; Connected Buildings; NIST; Identify; Protect; Detect; Respond; Recover*

I. INTRODUCTION

Smart buildings are increasingly adopting automation and connecting to the Internet, creating an energy-internet-of-things (EIOT) environment that converges operational technology (OT) and information technology (IT). Today, buildings increasingly weave together networked sensors and cyber and physical systems that enable big 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 nodes, it becomes more difficult to protect the security of the data life cycle. 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—not cybersecurity.

The Buildings Cybersecurity Framework (BCF) [1] is a product of a collaborated effort between the U.S. Department of Energy's Pacific Northwest National Laboratory and EERE's Building Technologies Office. BCF applies to six of the sixteen critical infrastructure sectors designated by the Department of Homeland Security, including commercial facilities (e.g., public assembly, offices, lodging), financial services (e.g., banking and insurance), government facilities, healthcare and public health, emergency services (e.g., fire and police stations), and information technology. Information Technology (IT) is the backbone of all businesses and some of the critical IT applications include managing critical data, controlling physical processes such as the power grid [2]. Therefore, securing the IT infrastructure and the (OT) networked devices is imperative in securing the building.

The Buildings Cybersecurity Framework (BCF) provides general guidance to building owners and operators to identify and implement a cybersecurity risk management strategy to secure critical buildings Information Technology (IT) and Operational Technology (OT). To realize this goal, the framework provides insight into common vulnerabilities, threats, and potential impacts from cyber-attacks. Securing buildings from emerging cyber threats is a process, not an end state. This process requires incorporating cybersecurity best policies, practices, and procedures. The Framework provides case studies and illustrations highlighting common cyber threats, vulnerabilities, and mitigation recommendations to reduce these vulnerabilities, ensure service reliability, and manage cyber risk.

The national opportunity and challenge to secure buildings from emerging cyber threats cannot be overstated. The recent documented findings in government reports [3]–[9], indicate the growing threat of physical and cyber-based attacks on electric grids and other critical infrastructure systems [10]. Buildings technology is increasingly digitized and connected to cyberspace, enabling new opportunities to increase interoperability, connectivity, and energy efficiency, and to use renewable energy. The nation's 5.6 million commercial buildings use 19% and 36% of the nation's primary energy and electricity use, respectively; Department of Energy's (DOE's) goal is to improve energy use per square foot in this sector by 30% by 2030, relative to 2010 [11]. Achieving this goal requires the secure development, deployment, and management of advanced building technology that is increasingly connected to the Internet and vulnerable to emerging cyber threats.

As the National Academies recently observed: "These systems provide critical services that allow a building to meet the functional and operational needs of building occupants, but

This study has been conducted at the Pacific Northwest National Laboratory is operated for the U. S. Department of Energy by the Battelle Memorial Institute under Contract DE-AC05-75RL01830.

they can also be easy targets for hackers and people with malicious intent. As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks." 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 smart grid incorporates smart metering and load management, which leads to high risk of user and corporate privacy by making things easily accessible and available to anyone; may motivate an attack on the power grid [12]-[16] (an attacker reducing electricity bill). While increasing cybersecurity awareness and risk management is essential, buildings vary greatly in the technology they deploy and the resources available to protect it.

In response, DOE's Building Technologies Office developed the Framework to provide easy to follow general guidance, drawn from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and a wide variety of industry best practices and guidance documents (i.e., NIST 800 series, DoD United Facilities Criteria) [17]. The Framework will facilitate buildings cybersecurity risk management efforts and help increase an organization's cybersecurity posture by identifying security gaps and providing energy managers and buildings personnel actionable guidance to help secure their buildings from various cybersecurity vulnerabilities and evolving cyber threats. The BCF is not a one-size-fits-all approach to managing cybersecurity risk for buildings. Buildings will continue to have unique cyber risks—different threats, vulnerabilities, and risk tolerances. While resources will help determine how users implement the BCF, it will help organizations determine activities that are important to critical service delivery and prioritize investments to maximize the effectiveness of security investments.

II. Buildings Cybersecurity Framework

A. BCF Overview

The BCF (also available as a web tool at cf.pnnl.gov) provides five concurrent and continuous functions (which can also be referred as Domains) to Identify, Protect, Detect, Respond, and Recover from cyber threats and vulnerabilities to buildings. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's cybersecurity risk management. The Framework, provides an easy to follow set of cybersecurity best practices, policies, and procedures to improve the cybersecurity posture of our nation's buildings. The Framework is also designed to facilitate communication of cybersecurity activities and outcomes across the organization from the executive to operations levels.

The BCF helps to realize the goals of the Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) [18], which calls on Federal agencies and critical infrastructure owners and operators to manage their cyber risk through adoption of The Framework for Improving Critical Infrastructure Cybersecurity (EO 13636) developed by the National Institute of Standards and Technology (NIST) in February 2014 [19].

BCF provides a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help building owners and operators better manage cybersecurity risks. BCF provides a common taxonomy and mechanism for buildings stakeholders to

- 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, and
- communicate among internal and external stakeholders about cybersecurity risk

B. BCF Features

- Practices, policies, procedures to guide cybersecurity activities & an organization's risk management processes.
- Detailed cybersecurity activities, outcomes, and informative references, providing detailed guidance for developing individual organizational risk profiles.
- Checklists and use cases to help building stakeholders align their cybersecurity activities with their business requirements, risk tolerances, and resources.
- Case studies providing real world examples of how to implement the best practices found in each chapter.

C. BCF Applications

The Buildings Cybersecurity Framework complements, but does not replace, an organization's existing risk management process and cybersecurity program. Building owners and operators can use their current processes and leverage the Framework to identify opportunities to strengthen their cybersecurity risk management and adopt industry best practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

III. Critical Domains of BCF

Following the core approach of the NIST Cybersecurity Framework, the BCF provides actionable functions that can be easily adopted by an organization operator to enhance the organization security. The essence is captured in a set of "how-to" instructions for organization operators to adopt, adapt, and apply to their respective organizations. BCF Core Functions are defined in Fig. 1.

Those 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 the dynamic cybersecurity risk.

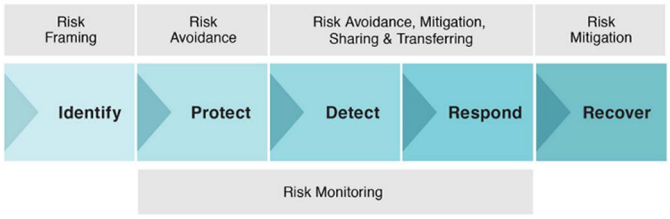

Fig. 1. Outline of Buildings Cybersecurity Framework

A. *Identify*

The goal of this 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 word, 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. CCAs (an illustration is shown in Fig. 2) are distinctively defined as Information Technology (IT) and Operational Technology (OT) that are connected to the operation of the organization and associated organizational goals. To realize the goal, various risk framing techniques are described to develop a risk characterization matrix. Activities in the Identify domain help building operators focus and prioritize efforts, consistent with its 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.

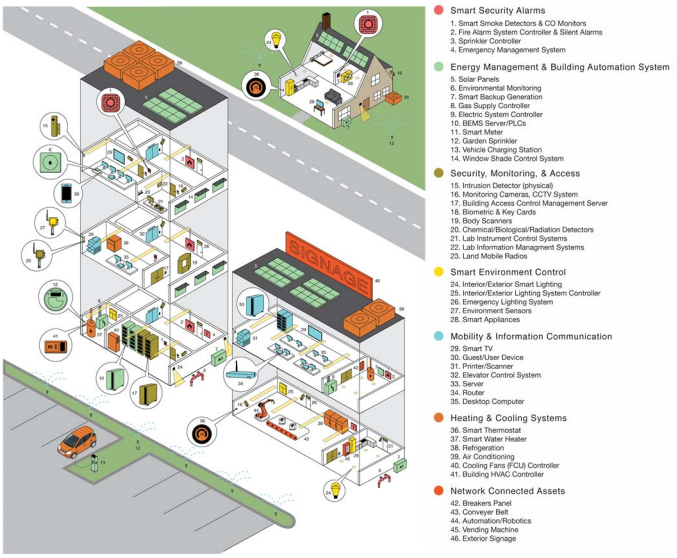

Fig. 2. Illustration of Common Critical Cyber Asssets Found in Buildings

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.

2) Business Environment: The oganization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

3) Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and opeartional requirements are understood and inform the management of cybersecurity risk.

4) Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

5) Risk Management Strategy: The organization's priorities, constraints, risk tolerances, and asumptions are established and used to support operational risk decisions.

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.

B. *Protect*

The goal of this function is to protect assets by introducing building operators to cyber protection techniques, as shown in Fig. 3, that enable risk control through risk avoidance. *Protect* will help operators develop and implement the appropriate safeguards to increase a building's cybersecurity posture. The Protect Function 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.

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.

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.

3) Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

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.

5) Maintenance: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

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.

Fig. 3. Key Protection measures to defend a building against cyber attacks

C. Detect

The goal of this 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 cyber-attack as depicted in Fig. 4.

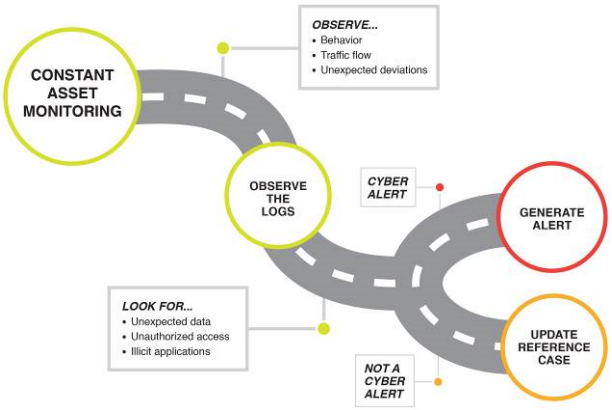

Fig. 4. Detection path towards concluding an anomaly as a cyberattack

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

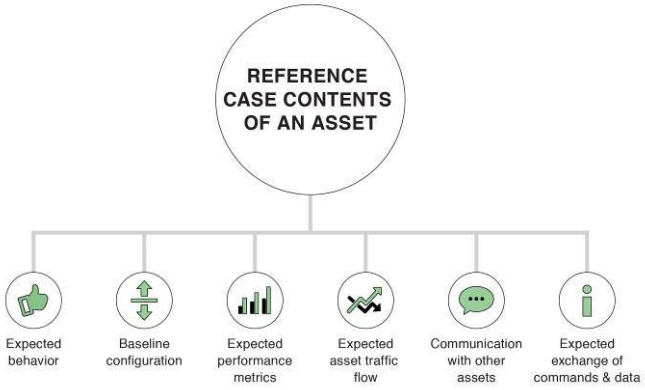

Fig. 5. Illustrative reference case for critical asstes

1) Anomalies & Events: Anomalous activity is detected in a timely manner. Potential impact of events is understood.

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.

3) Detection Processes: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

D. Respond

The goal of this function is to respond to a cyber-attack 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 building operators to know the best course of action to minimize impact.

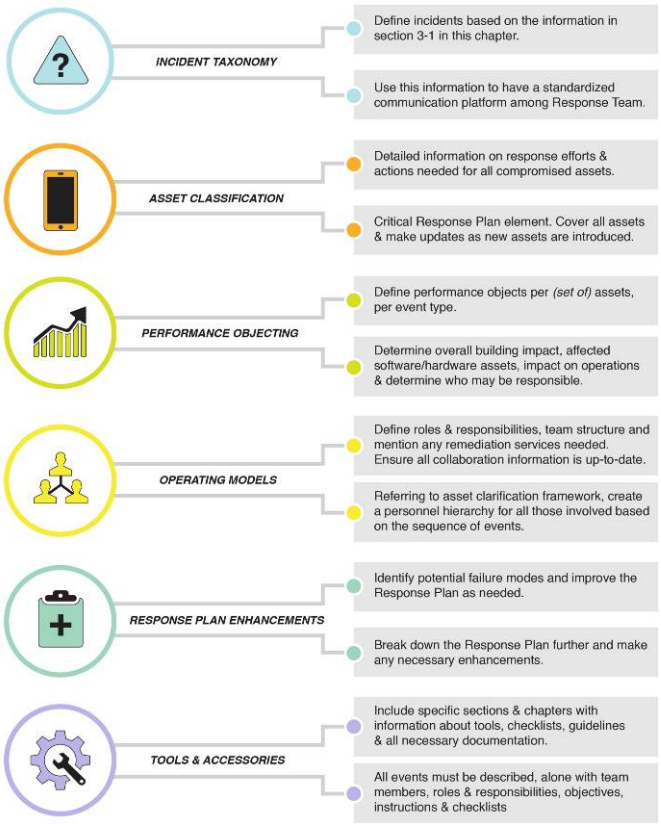

Fig. 6. Critical contents of a Cybersecurity Response plan

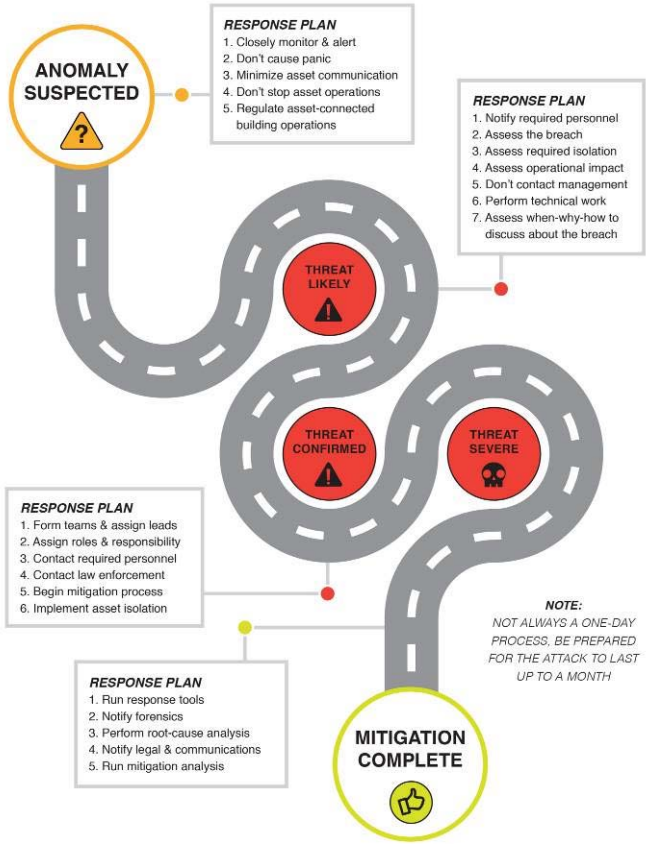

Fig. 7. Implementation path of a response plan post cyber intrusion detection

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

1) Response Planning: Response processes and procedures are executed and maintained, to ensure timely response to detect cybersecurity events.

2) Communication: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

3) Analysis: Analysis is conducted to ensure adequate response and support recovery activities.

4) Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

5) Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

E. Recover

The goal of this function is to recover and return services to normal operation and reduce the impact of a cybersecurity event. *Recover* provides insight on the creation and implementation of a recovery plan for building operators. This plan will include solutions to recover compromised buildings 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.

1) Recovery Planning: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

2) Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

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.

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. Establish 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 –
    a. Identify mission commander priorities. Then identify dependencies and develop reintegration sequence.
    b. Reintegrate clean assets. Ensure that the assets are infection-free. Integrate the subsystem and the network layers.
    c. Finally, the recovery phase should monitor the reintegrated components to ensure all evidence of the cyber incident has been eliminated from the network.
8. Note that the recovery plans specific to assets can be found in ICS – Servers/workstations

IV. Inherent Frameworks and Standards in Buildings Cybersecurity Space

Buildings Cybersecurity framework is arranged as chapters where each cover one of the five functions of the BCF in sequence. Each chapter includes illustrative figures and visualizations that building operators can employ to make function-specific enhancements to their buildings. In addition, for demonstration purposes, the flowcharts are applied to example building models at the end of each chapter, to demonstrate the use of the BCF.

Buildings-focused BCF was developed based on a careful review and adaptation of cybersecurity best practices for buildings. The BCF core is based on the five core elements of the NIST Cybersecurity Framework for Critical Infrastructure. In addition to the Framework, BCF provides an overlay of cyber best practice and standards documents, including: The Buildings Cybersecurity Maturity Model (B-C2M2) [20], NIST 800-53 R4 [21], NIST 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015 [22], SANS Institute 20 Critical Security Controls [23] and DoD Facility-Related Control Systems Cybersecurity Guidelines [17]. Additional guidance and best practice were also leveraged from the following best practices and standards documents:

- SANS Institute 20 Critical Security Controls [23]
- ISA 62443-3-3:2013 [24]
- ISO/IEC 27001:2013 [25]
- DOE Cybersecurity Capability Maturity Model [26]
- DOE Buildings Cybersecurity Maturity Model [20]
- DOE's U.S. Department of Defense, Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems (UFC) [17]
- CNSSI 1253, Security Categorization and Control Selection for National Security Systems 2014 [27]
- Department of Defense (DoD) Instruction 8500.01, Cybersecurity [28]
- DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) [29]
- DoD Industrial Control Systems Advanced Tactics, Techniques and Procedures Jan 2016 [30]
- DoD Facility-Related Control Systems Cybersecurity Guidelines [17]
- National Institute of Standards and Technology Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations 2013 [21]
- National Institute of Standards and Technology Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015 [22]
- National Institute of Standards and Technology Special Publication SP 800-115 [31]
- Unified Facilities Criteria 3-410-01 Utility Monitoring and Control System (CS) Front End and Integration 2016 (DRAFT)
- Unified Facilities Criteria 3-410-02 Direct Digital Control for HVAC and Other Building Control Systems [32]
- Government Accountability Office Report 15-6 Federal Facility Cybersecurity 2014 [33]
- DoD Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations [34]

Acknowledgement

The authors would like to acknowledge the editorial contribution of Sraddhanjoli Bhadra.

Conclusion

This paper provides an overview of the Buildings Cybersecurity Framework (BCF). The BCF foundation is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Critical Infrastructure. BCF has five major operations: identify, protect, detect, respond and recover – each of which details the methodologies to mitigate cybersecurity risk in a building. It is applicable to wide variety of buildings, including: residential, small, medium, large commercial and federal buildings. The identify function identifies cyber security threats and vulnerabilities. Based on the identification, the protect function introduces protection recommendations to manage cyber risk. The detection function focuses on techniques, policies and procedures to detect anomalies and attacks. The respond chapter highlights, a set practices to effectively respond to cybersecurity event. Finally, the recover function focuses on returning services to their normal operations and mitigate the

damage caused by the cybersecurity incident. Implementing the BCF will help buildings stakeholders manage their cyber risk. In addition, the BCF provides an effective process to help realize the goals of recent helps to realize the goals of the Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017), which calls on Federal agencies and critical infrastructure.

REFERENCES

[1] Joe Haggerman, Michael Mylrea, Sri Nikhil Gupta Gourisetti, Andrew Nicholls, "Buildings Cybersecurity Framework", PNNL-EERE Working Draft (Forthcoming) 2017.

[2] H. Holm et al., "P^{2}CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language", *IEEE Transc. on Dependable and Secure Computing*, vol. 12, no. 6, Nov.-Dec. 1, 2015.

[3] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, "Roadmap to Secure Control Systems in the Energy Sector", January 2006. [Online]. Available: http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf

[4] Supervisory Control and Data Acquisition (SCADA) Systems, Nat. Commun. Syst., Arlington, VA, Oct. 2004. [Online]. Available: http://www. ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[5] Critical infrastructure protection report, Government Accountability Office, Washington, DC, May 2005. [Online]. Available: http://www.gao.gov/new.items/d05434.pdf

[6] Challenges and Efforts to Secure Control Systems, Government Accountability Office, Washington, DC, Mar. 2004. [Online]. Available: http://www.gao.gov/new.items/d04354.pdf

[7] M. R. Permann and K. Rohde, Cyber Assessment Methods for SCADA Security, Research Triangle Park, NC: Instrum. Soc. Amer. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/Cyber_Assessment_Methods_for_SCADA_Security_Mays_ISA_Paper.pdf

[8] R. E. Carlson, J. E. Dagle, S. A. Shamsuddin, and R. P. Evans, A Summary of Control System Security Standards Activities in the Energy Sector, DC: U.S. Dept. Energy, Office Electricity Delivery Energy Reliab., Nat. SCADA Test Bed (NSTB), Oct. 2005. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/Control_System_Security_Standards_Activities.pdf

[9] Information Security: Technologies to Secure Federal Systems, Mar. 2004, Report to Congressional Requesters, GAO-04-467. [Online]. Available: http://www.gao.gov/new.items/d04467.pdf

[10] C. Ten et al., "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling", *IEEE Transc. on Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol. 40, no. 4, July 2010.

[11] U.S. Department of Energy Building Technologies Office, "Multi-Year Program Plan", Jan. 2016. [Online]. Available: https://energy.gov/sites/prod/files/2016/02/f29/BTO_MYPP_2016.pdf

[12] J. Liu et al., "Cyber Security and Privacy Issues in Smart Grids", *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4.

[13] H. Khurana et al., "Smart-grid security issues", *IEEE Security & Privacy*, vol. 8, no. 1, Jan-Feb 2010.

[14] X. Li et al., "Securing smart grid: cyber attacks, countermeasures, and challenges", *IEEE Communications Magazine*, vol. 50, no. 8, August 2012.

[15] Y. Mo et al., "Cyber-Physical Security of a Smart Grid Infrastructure", *Proc. IEEE*, vol. 100, no. 1, Jan. 2012.

[16] U. S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," NIST IR-7628, Aug. 2010. [Online] available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[17] U. S. Department of Defense, "Unified Facilities Criteria (UFC): Cybersecurity of Facility-Related Control Systems", January 2017 [Online]. Available: https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf

[18] The White House, "Presidential Executive Order on Strengthning the Cybersecurity of Federal Networks and Critical Infrastructure", May 2017. [Online] Available: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[19] U. S. NIST, "Framework for Improving Critical Infrastructure Cybersecurity", February 2014. [Online] Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[20] U. S. Department of Energy, "Buildings Cybersecurity Maturity Model (B-C2M2)", [Online]. Available: https://bc2m2.pnnl.gov/

[21] U. S. NIST, "Security and Privacy Controls for Federal Information Systems and Organizations", Apr. 2013 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[22] U. S. NIST, "Guide to Industrial Control Systems (ICS) Security", May 2015. [Online] Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[23] The Center for Internet Security (CIS) Critical Security Controls V6.0 [Online]. Available: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

[24] NIST Cybersecurity Framework Core: Informative Reference Standards, April 2014 [Online]. Available: https://www.americanbar.org/content/dam/aba/administrative/law_national_security/nistframework/NIST%20Cybersecurity%20Framework%20Core%20-%20ISA%2062443-3-3-2013.authcheckdam.pdf

[25] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements [Online]. Available: http://www.iso27001security.com/html/27001.html

[26] U. S. Department of Energy and U.S. Department of Homeland Security, "Cybersecurity Capability Maturity Model (C2M2)", February 2014. [Online]. Available: https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[27] Committee of National Security Systems (CNSS), "Security Categorization and Control Selection for National Security Systems", March 2014 [Online]. Available: http://www.dss.mil/documents/CNSSI_No1253.pdf

[28] U. S. Department of Defense, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle", Sept. 2015. [Online]. Available: https://www.dau.mil/tools/Lists/DAUTools/Attachments/37/DoD%20-%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf

[29] U. S. Department of Defense Instruction, "Risk Management Framework (RMF) for DoD Information Technology (IT), May 2016 [Online]. Available: https://www.hsdl.org/?abstract&did=793050

[30] U. S. Department of Defense, "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)", Jan. 2016 [Online] Available: http://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS.pdf

[31] U. S. NIST, "Technical Guide to Information Security Testing and Assessment", Sept. 2008. [Online] Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[32] U. S. Department of Defense, "Unified Facilities Criteria (UFC): Direct Digital Control for HVAC and Other Local Building systems", July 2013. [Online] Available: https://www.wbdg.org/FFC/DOD/UFC/ufc_3_410_02_2012_c1.pdf

[33] Governement Accountability Office Report, "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems", Dec. 2014. [Online]. Available: http://www.gao.gov/assets/670/667512.pdf

[34] U. S. Department of Defense, "Handbook for Self-Assessing Security Vulnerabilites and Risks of Industrial Control Systems on DOD Installations", December 2012 [Online]. Available: https://www.wbdg.org/files/pdfs/ics_handbook.pdf