Please find attached GSA's Office of Federal High Performance Buildings' response to the NICE framework Request for Comments for your consideration.

Thank you,
Maureen K. Roskoski, CFM, SFP, ProFM, LEED AP O+M, ISO 22301 Lead Auditor
Senior Professional, Corporate Sustainability Officer

Facility Engineering Associates, PC | **www.feapc.com**
12701 Fair Lakes Circle, Suite 101, Fairfax, Virginia 22033|Office.703-591-4855

FEA…Improving the Way You Manage Facilities

January 13, 2020

NICE Framework Request for Comments Response from GSA's Office of Federal High Performance Buildings

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is planning to update the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181 and has invited the public to provide input for consideration in the update. The GSA's Office of Federal High Performance Buildings has reviewed the requested considerations for the public comment response and submits this summary.

GSA recommends that NIST add facility management, energy management, and facility operations roles to the NICE framework. GSA reviewed the existing NICE framework and only found one work role, Program Manager, that might be relevant to the facilities positions. We mapped the FBPTA cybersecurity competencies to the NICE work role of Program Manager and found six of the nineteen competencies aligned with the competencies identified in the NICE framework. This mapping exercise revealed that the current work categories do not cover facilities roles.

Over the past few decades, the tools for managing buildings have substantially changed, and today facility managers, energy managers and building operators are more dependent on digital technologies to run buildings and monitor efficiency and costs. While technology has improved exponentially during the last 10 years, providing building managers with excellent and more sophisticated tools, it has also brought an increased threat of disruption through cyber-attacks. This threat requires facilities personnel to obtain and maintain competencies related to cyber security for facility systems, subsystems, sensors, and other devices. In 2018, the Facilities Management Institute (FMI) through its Federal Buildings Personnel Training Act (FBPTA) program added cybersecurity competencies to its competency model for Facility Management, Energy Management, and Facility Operations roles to meet these needs.

FMI convened a working group of federal agency representatives to determine cybersecurity competencies appropriate for facilities personnel. This working group contained representatives from Department of Defense (DoD), National Institute of Science and Technology (NIST), General Services Administration, National Academies of Science, and private industry representatives. The working group met several times, conducted discussion, and achieved consensus on 19 competencies related to cybersecurity in the facilities realm. These competencies were included as performances in the FBPTA competency model in the Technology competency area, broken up into two core competencies: Cybersecurity in Facility Management and Building O&M and Cybersecurity in Design and Acquisition. The purpose of these additional performances is to clarify the role facilities personnel play related to cybersecurity and to identify curriculum to meet those competencies. These competencies developed by a diverse working group can be utilized as the foundation for the content within the NICE framework for the facilities roles.

Education of the facilities personnel who deal with many building systems that are vulnerable to cyber-attacks can greatly enhance the security of an organization.

Included in Appendix A are the FBPTA cybersecurity competencies.

Contact Maureen Roskoski at maureen.roskoski@feapc.com for more information
Submitted on behalf of GSA Office of Federal High Performance Buildings

FBPTA Cybersecurity Competencies

Competency Areas (1)	New Cybersecurity Core Competencies (2)	New Cyber Performances (19)	Performance Additional Comments	Role Competency	Cyber-Security Focused Training Resources
	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	**Facility Manager, Energy Manager**	ICS-CERT: Intro to Control Systems Cybersecurity NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab
		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.	**Facility Manager, Energy Manager**	ICS - CERT: Intermediate Cybersecurity for Industrial Controls Systems, NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, Network Penetration Testing and Computer Networks CS 420: Data Communications ICS-CERT: ICS Cybersecurity Scadahacker: General ICS and Cybersecurity Training NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab SANS: Defending ICS Servers and Workstations Infosec: Scada Security Online ISA.org: Cyber Security for Automation, Control and SCADA systems. isa.org: Cyber Security for Automation, Control and SCADA Systems NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions USMA: Information Warfare Analysis Research Laboratory (IWAR) Network Penetration Testing and Computer Networks ICS-CERT Cyber Security Industrial Control Systems SANS: FOR508 Advanced Digital Forensics and Incident Response & NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, Tulsa: Malware Analysis and Creation
		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 system. Policies should include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization.	**Facility Manager, Energy Manager, Facility Operator**	NIBS: Cybersecuring DoD Control Systems Workshop ICS CERT: Intro to Control Systems Cybersecurity NIBS: Advanced Cybersecuring DoD Control Systems Workshop ISA.org: Cyber Security for Automation, Control and SCADA systems Process for planning remedial actions (Partial): CS4684 Cyber Security Incident Response and Recovery may cover some aspe
		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.		**Energy Manager**	
		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.	**Facility Manager, Energy Manager, Facility Operator**	Infosec Institute: Security Boot Camp, SANS: Defending ICS Servers and Workstations SANS: FOR508 Advanced Digital Forensics and Incident Response & MGT535 Incident Response Team Management NPS: 26 Security Adversarial Techniques Certificate, CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation ICS-CERT: Intermediate Cybersecurity for ICS NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab
		3.4.6. Demonstrate knowledge of how to perform continuous monitoring of control systems and identify system instability.		**Facility Manager, Energy Manager, Facility Operator**	isa.org: Cyber Security for Automation, Control and SCADA Systems (IC32E) NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab
		3.4.7. Demonstrate knowledge of control systems' and recognizing abnormal behavior and anomalies.		**Facility Manager, Energy Manager, Facility Operator**	*No Training available Not directly focused on anomaly detection and baselining, but may be relevant: ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems
		3.4.8. Demonstrate knowledge of procedures for maintaining authority to operate (ATO) building systems	Federal specific performance	**Energy Manager**	*NIST: Industrial Control Systems (ICS) Security Workshop

FBPTA Cybersecurity Competencies

		New Cyber Performances (19)	Performance Additional Comments	Role Competency	Cyber-Security Focused Training Resources
3. Technology		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	**Facility Manager, Energy Manager, Facility Operator**	ICS-CERT: Operational Security (OPSEC) for Control Systems ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems SANS: FOR508 Advanced Digital Forensics and Incident Response MGT535 Incident Response Team Management NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation InfoSec: SCADA/ICS Security Boot Camp Scadahacker: General ICS and Cybersecurity Training: *NIST: ICS Workshop May also be relevant: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory
		3.4.10. Demonstrate knowledge of cyber security technologies in accordance with relevant regulatory requirements, including hardware, software, and firmware.		**Energy Manager**	ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems SANS: Defending ICS Servers and Workstations Infosec: Scada Security Online ISA.org: Cyber Security for Automation, Control and SCADA systems.
		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.		**Facility Manager, Energy Manager**	
	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.		**Facility Manager, Energy Manager**	
		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 where long-term operations and maintenance is conducted by third parties.	**Facility Manager, Energy Manager**	NIBS: Cybersecuring DoD Control Systems Workshop AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions Tulsa: Software Reverse Engineering, Network Penetration Testing and Computer Networks CS3030 Computing Architecture and Operating Systems, Software Engineering and Architecture, and Information Security S Engineering (ISSE)
		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	**Facility Manager, Energy Manager**	*No Training available May be addressed in part by: NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions Tulsa: Software Reverse Engineering, Network Penetration Testing and Computer Networks AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory NIBS: Cybersecuring DoD Control Systems Workshop
		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	**Energy Manager**	
		3.5.5. Demonstrate familiarity with incorporating cybersecurity requirements into lease language and occupancy agreements for systems, subsystems, sensors, and other component devices.		**Facility Manager, Energy Manager**	*No Training available
		3.5.6. Demonstrate ability to identify, address, and escalate issues where new emerging technologies and cybersecurity requirements affect costs and budgeting.		**Energy Manager**	NIBS: Cybersecuring DoD Control Systems Workshop ISU: EE 447 Digital Signal Processing NMT: CSE 452 Sensor Networks isa.org: Cybersecurity for automation, control and SCADA systems. NPS: RES 261 Cyber Security Adversarial Techniques Certificate, CS3030 Computing Architecture and Operating Systems, Sof and Architecture, and Information Security Systems Engineering (ISSE) USMA: Computer Architecture UI: CS451 Advanced Computer Architecture

		New Cyber Performances (19)	Performance Additional Comments	Role Competency	Cyber-Security Focused Training Resources
		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	**Facility Manager, Energy Manager**	*No Training available
		3.5.8. Demonstrate ability to recognize and understand the role of cyber security requirements in the ecosystem of integrated project delivery.		**Facility Manager, Energy Manager**	SANS GAIC: ICS Security Governance