Naval Facilities Engineering Systems Command
NAVFAC Hawaii

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

Julie Weinstein, NAVFAC HI CIO

January 10, 2024

Overall Classification: UNCLASSIFIED

Disclaimer

DISCLAIMER: Although the subject matter of the following presentation deals with an ongoing or announced program by the Department of Defense, the views presented here are those of the speaker and DO NOT necessarily represent the views of the Department of the Navy, DoD or its components.

Reference: 5 CFR 3601.108

UFC 4-010-06

Cybersecurity of Facility-Related Control Systems

“This UFC describes requirements for incorporating cybersecurity in the design of all facility-related control systems which include a network. This UFC covers the cybersecurity aspects of control system design, and the requirements of this UFC must be coordinated with the control system design and the criteria relevant to the control system. This UFC only covers aspects specific to control system design. Many projects have IT-specific components (such as IP network design security) which are not covered by this UFC; in those cases, the controls designer will need to coordinate with other disciplines. This UFC defines a process for identification of cybersecurity requirements based on the Risk Management Framework suitable for control systems of any impact rating and provides specific guidance suitable for control systems assigned LOW or MODERATE impact level.”

NAVFAC HI CIO

- **CIO2 Cybersecurity (RMF) and CIO4 Facility-Related Control Systems Cybersecurity (CSPE)**
  - –Work with Planning Division to determine estimated cybersecurity costs: Contractor and Government
    - Anticipate a reduction in contractor design and RMF support
  - –Work with Design and Construction PMs to capture cybersecurity requirements:
    - Connect to CSPE: Determine closest POP
    - Follow existing Public Works J&A
    - Determine/design cybersecurity strategy: 25 05 11, MFR or ATO
  - –Execute ISSM/ISSO roles/responsibilities during RMF
  - –Configure CSPE networking equipment and/or servers to connect the system.

Highlights

“Good cybersecurity design is best accomplished via good control system design”

- 2.2 5 Level Control System Architecture
- RMF is IT-centric. Must articulate why a control can be or cannot be implemented and if not, how the risk can be mitigated. This requires a strong technical understanding or your control system hardware, software and operations
- Read and follow the guide spec! “The design specifications for control system cybersecurity developed in accordance with this UFC must derive from UFGS 25 05 11.”
  - –UFGS 25 05 11 –coordinate with other disciplines

Recommendations for Success

- **Engage with the PM about cybersecurity early in the project!**
  - –The PM is you POC and method to contact CIO
  - –Provide Hardware/software list early for review
- **Learn our language. The UFC and UFGS are “translations”**
  - –National Standards and Technology (NIST) Special Publication (SP) 800-37 R2, *The Risk Management Framework*
  - –NIST 800-82 R2, *Guide to Industrial Control Systems (ICS) Security*
  - –NIST 800-53 R5*, Security and Privacy Controls for Federal Information Systems and Organizations. 800-53A R5.1.1 & 800-53B*
  - –Committee of National Security Systems (CNSS) Policy 22
  - –CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*
- **Focus on technical controls. Know how your FRCS can be “hardened”**
- **Know the mission. It will impact the CYBERSAFE grade. CYBERSAFE Systems require a full ATO!** It will also determine the level of stringency for the cybersecurity controls that will be implemented.
- **Our systems are unique –** Do not “cut and paste” from what you have done before. Ask questions!

Recommendations cont…

- **Cyber Workforce Requirements apply to contractors** **SECNAVINST 5239.25**
- **Security clearance requirements apply to contractors** **SECNAVINST 5510.30C**
- **Find or develop your FRCS Cybersecurity experts:**
  - Know the control system
  - Know how to "harden" or secure it
  - Know how to communicate its cybersecurity posture to the government