ENGINEERING AND CONSTRUCTION BULLETIN

US Army Corps of Engineers

No. 2022-2 **Issuing Office:** CECW-EC **Issued:** 07 Jan 22 **Expires:** 07 Jan 24

SUBJECT: Cybersecurity Requirements for Design and Construction of Control Systems and Integrated Low Voltage Systems for Permanent and Non-permanent Construction

CATEGORY: Directive and Guidance

1. **References**:

a. Unified Facilities Criteria (UFC) 4-010-06 Change 1, Cybersecurity of Facility-Related Control Systems, 18 January 2017

b. Unified Facilities Guide Specification (UFGS) 25 05 11, Cybersecurity for Facility-Related Control Systems, 1 November 2017

c. Unified Facilities Criteria (UFC) 1-201-01, Non-Permanent DoD Facilities in Support of Military Operations, 01 January 2013

d. Headquarters Department of Army (HQDA) Execution Order (EXORD) 141-18, 18 Apr 2018, subject: Facility-Related Control Systems (FRCS) Cybersecurity

e. Fragmentary Order (FRAGO) 1 to HQDA EXORD 141-18, 14 Apr 2020

f. ECB 2019-9, Usage of The Unified Facilities Guide Specifications on USACE Projects, 03 May 2019

g. ER 25-1-113, USACE Critical Infrastructure Mandatory Center of Expertise (UCIC-MCX), 31 January 2019

h. ECB 2020-10, Facility-Related Control System Cybersecurity Coordination Requirement, 06 August 2020

i. ER 1110-1-8174 Military Programs Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX)

2. **Purpose.** This ECB provides direction and guidance for the mandate to use UFC 4-010-06 and UFGS 25 05 11 for all control systems designed or constructed by USACE, including those for USACE Civil Works. This ECB also clarifies USACE's design and construction roles and responsibilities related to control system cybersecurity.

3. **Applicability.** This ECB applies to all control systems designed or constructed by USACE for permanent or non-permanent facilities regardless of project type and funding source (e.g. Civil Works, Military Construction, Sustainment Restoration and Modernization, Interagency and International Services). This ECB also applies to all low-voltage systems which are designed or constructed by USACE for permanent or non-permanent facilities and which

integrate with control systems, regardless of project type and funding source for both permanent and non-permanent facilities.

4. **Background.**

a. The DoD requires applying the Risk Management Framework (RMF) to all control systems. Using a risk-based approach, the RMF process allows System Owners (in coordination with the Authorizing Official) to tailor cybersecurity requirements to meet mission and functional requirements.

b. UFC 4-010-06 defines the design process for incorporating cybersecurity into control system design in support of the RMF process. This design process is universal for all control systems and includes the identification of cybersecurity requirements to incorporate into design in coordination with the System Owner. The UFC also defines required design submittals, coordinated with the System Owner, to ensure that the design is meeting the owner's requirements.

c. USACE needs to clarify the required use of UFC 4-010-06 when designing Civil Works control systems and how the UFC aligns with the established Civil Works Operational Technology Cybersecurity Program.

d. There are instances where USACE is constructing a non-FRCS control system (e.g. a manufacturing system), or a low-voltage system which will be integrated with a control system (e.g. Nurse Call System). The process defined by UFC 4-010-06 for inclusion of cybersecurity in the design will apply to these systems, and the overall UGS 25 05 11 specification structure, requirements, and deliverables will largely be applicable as well.

e. Cybersecurity requirements apply to control systems for both permanent and non-permanent facilities. UFC 1-201-01, Non-Permanent DoD Facilities In Support of Military Operations, is currently undergoing revision and will incorporate UFC 4-010-06 as a requirement.

5. **Directive.**

a. USACE E&C is responsible for including cybersecurity requirements into the design of control systems in accordance with UFC 4-010-06 and System Owner requirements. USACE E&C is also responsible for the construction of systems in accordance with the design and the testing required to demonstrate compliance with the design. All other aspects of the RMF process remain the responsibility of the System Owner.

(1) Pursuant to ER 25-1-113 (reference g), the USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise (UCIC-MCX) provides cybersecurity design requirements for all System Owners of Civil Works and USACE-owned and operated control systems and performs cybersecurity design reviews for those systems. UCIC-MCX actively collaborates with Engineering & Construction (E&C) in regards to control system cybersecurity criteria.

(2) The project sponsor who is responsible for the operation of the infrastructure will provide the cyber requirements when USACE E&C is designing or constructing for external asset owners (military infrastructure). For such projects, the Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX) performs design reviews. If necessary, the CSC-MCX can facilitate the determination of asset owner requirements (ref h and i).

b. The System Owner is responsible for developing RMF artifacts (e.g. System Security Plan, Incident Response Plan) that are beyond the project submittals defined in UFC 4-010-06. The System Owner is also responsible for fulfilling all additional requirements necessary for obtaining an RMF Authorization to Operate (ATO).

(1) Pursuant to reference g, the UCIC provides direction and guidance for all RMF requirements, including RMF implementation processes and required RMF artifacts and documentation, for all System Owners of Civil Works and USACE owned and operated control systems.

(2) For Military projects, USACE may support System Owners with RMF ATO efforts, such as the development of artifacts and security engineering of non-control system components, on a reimbursable basis using contract or in-house resources when requested and funded.

c. All control systems, and other low-voltage systems integrated with control systems, designed and constructed by USACE for permanent and non-permanent facilities for both Civil Works and Military infrastructure will be designed in accordance with UFC 4-010-06 and cybersecurity requirements provided by the System Owner.

d. All control systems, and other low-voltage systems integrated with control systems, designed and constructed by USACE for permanent and non-permanent facilities for both Military and Civil Works infrastructure will use UFGS 25 05 11 as the starting guide specification for cybersecurity. The UFGS must be tailored to generate a project specification according to specific mission requirements. The UFGS 25 05 11 does not (currently) have Civil Works specific control system requirements and must be adapted by designers when used for these systems.

e. For Military Programs: Existing projects which include control systems but did not include UFC 4-010-06 and which have not completed design (i.e. acceptance of final design) must incorporate UFC 4-010-06 into the design.

f. For Civil Works:

(1) New project designs starting after the date of publication of this ECB must follow the UFC. For the purpose of this requirement, contracted designs start at Request for Proposal (RFP) issuance.

(2) Projects including Building Control Systems (e.g. HVAC, lighting), Fire Protection Systems, or Electronic Security Systems must use UFGS 25 05 11 to prepare project specifications for those systems.

(3) Projects including systems other than Building Control Systems, Fire Protection Systems or Electronic Security Systems, which start on or after June 1, 2023 or after the release of a UFGS 25 05 11 incorporating tailoring options for those systems, whichever comes first, must use UFGS 25 05 11 to prepare project specifications for those systems. Until that time, the District Chief of Engineering and Construction[1] has the authority to determine the appropriate specification for use on those systems. The use of UFGS 25 05 11, with appropriate project-specific modifications and enhancements, is encouraged in order to standardize specification approach and deliverables across all USACE design and construction.

g. Users of the UFC and UFGS who identify errors in or enhancements to the documents are encouraged to submit Criteria Change Requests via the document page on the Whole Building Design Guide website (https://www.wbdg.org/) or using the CCR submission page for the document:

- UFC 4-010-06: http://cms.wbdg.org/ccrs/new?ufc=4-010-06
- UFGS 25 05 11: http://cms.wbdg.org/ccrs/new?ufgs=25%2010%2010

6. **Point of Contact.** HQUSACE point of contact for this ECB is Joseph Bush, CECW-EC, 217-373-4433, Joseph.Bush@usace.army.mil.

//S//
PETE G. PEREZ, P.E., SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers

[1] For Districts and Centers without a Chief of Engineering and Construction, the responsibility is assigned to the Chief of Engineering