ENGINEERING AND CONSTRUCTION BULLETIN

US Army Corps of Engineers

No. 2020-10 **Issuing Office:** CECW-EC **Issued:** 06 Aug 20 **Expires:** 06 Aug 22

SUBJECT: Facility-Related Control System Cybersecurity Coordination Requirement

CATEGORY: Directive and Guidance

1. **References**:

a. Army Regulation (AR) 25-1, Army Information Technology, 25 July 2013

b. AR 25-2, Information Assurance, 24 October 2007, Rapid Action Revision (RAR), 23 March 2009

c. Department of Defense Instruction (DODI) 8500.01, Cybersecurity, 14 March 2014

d. DODI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014

e. National Institute of Standards and Technology (NIST) Special Publication 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, February 2015

f. NIST Special Publication 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, April 2013

g. NIST Special Publication 800-53A Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans, December 2014

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

i. FY18-22 USACE Campaign Plan, 01 June 2017

j. Appointment Memorandum 16-01, Appointment of the Civil Works Control Systems National Information System Security Manager (ISSM-N), and the Critical Infrastructure Cyber Security Center of Expertise (CICS-MCX), 15 December 2016

k. Industrial Control Systems (ICS) Cybersecurity Technical Center of Expertise (TCX) Charter, 5 December 2014

l. Director, Military Programs Memorandum, USACE Guidance on Industrial Control Systems (ICS) Cybersecurity for Military Programs, 31 March 2016

m. ER 25-1-113, USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise, 31 January 2019

2. **Purpose.** This ECB provides direction and guidance for the mandate to coordinate cybersecurity requirements for all facility-related control system projects executed by USACE for external stakeholders.

3. **Applicability**

a. This ECB applies to all facility-related control systems (FRCS) designed and constructed by USACE for external stakeholders, including but not limited to: utility control systems, building control systems, electronic security systems, utility monitoring control systems (UMCS) and fire and life safety systems.

b. Note that control systems which are USACE owned must coordinate with the USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise in accordance with reference m.

4. **Background**

a. Facilities and Installations are platforms for mission readiness. Increasingly, these assets rely on automated and, in many cases, networked control systems to support real-time centralized monitoring and operations, making them vulnerable to cyber-attack. USACE must embrace cybersecurity to assure the confidentiality, integrity, and availability of these control systems that underpin its facilities and national critical infrastructure.

b. USACE plays a vital role in planning, engineering, designing and construction management for the Army and other entities throughout Military Programs (MP), work for others (WFO), Support for Others (SFO), and Environmental Programs. To support the cybersecure design and construction of facility-related control systems a mandatory center of expertise has been established to support projects executed for external stakeholders.

c. The Control Systems Cybersecurity Mandatory Center of Expertise (CSC-MCX) supports design and construction of functional and cyber-secure control systems. It was established to oversee and track consistent application of cybersecurity requirements by Districts, Centers, and Major Subordinate Commands. The CSC-MCX is located at the Engineering and Support Center, Huntsville.

5. **Directive**

a. Until the ER governing the CSC-MCX is released, coordinate cybersecurity design with the CSC-MCX in accordance with the mandatory function list in Attachment (1) for projects that include control systems and for which one or more of the following apply:

(1) The project is MILCON (including Unspecified Minor Military Construction (UMMC).

(2) The project is a Sustainment, and Restoration and Modernization (SRM) project related to Task Critical and or Defense Critical Asset.

(3) The project is an SRM project with requirements related to FRCS, and the estimated design and construction cost related to FRCS is greater than $250,000.

(4) The project is an Interagency and International Services (IIS) project with requirements related to FRCS, and the estimated design and construction cost related to FRCS is greater than $250,000.

(5) The project is deemed critical by the end user / requirement generator (where the control system confidentiality, integrity or availability has an impact rating of HIGH).

(6) The end user / requirement generator specifically requests the use of the CSC-MCX.

b. Costs for the coordination of cybersecurity design is on a reimbursable basis; provide project funding to CSC-MCX for these services. After the ER governing the CSC-MCX is released, coordinate cybersecurity design with the CSC-MCX in accordance with the ER. Provide project funding to CSC-MCX for these services in accordance with the ER.

c. These reporting and coordination requirements are in addition to existing requirements for reporting and coordination with the appropriate control system Mandatory Centers of Expertise (MCX).

d. USACE Districts, Centers, and Major Subordinate Commands retain responsibility for executing the design and installation of functional, cyber-secure control systems, with respect to applicable policies, customer requirements, and design criteria.

e. Additional coordination and collaboration with the CSC-MCX is always encouraged. In addition to the mandatory services, the centers provides guidance and technical support services on a reimbursable basis. For example, the CSC-MCX can provide additional support for: design, acquisition, construction quality control and system testing.

f. The CSC-MCX point of contact for this action is the CSC-MCX Technical Director, CEHNC-EDS-I, 256-895-1153 or CSC-MCX@usace.army.mil.

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//
CHRISTINE T. ALTENDORF, P.E., PHD, SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers

Encl.
Attachment 1 – CSC-MCX Mandatory Services

ATTACHMENT 1: CSC-MCX Mandatory Services

For each project required by the ECB to coordinate with the CSC-MCX, the following CSC-MCX services are mandatory:

(1) Provide final certified FRCS cybersecurity costs and parametric design review in support of the DD 1391 review and certification process for Military Construction-Army projects.

(2) Participate in advanced planning activities and design charrettes for projects that involve the application of FRCS systems security engineering and cybersecurity, including performing cybersecurity site surveys.

(3) Review design submittals (i.e., 35%, 65%, 95%, and final). Review of design documents will consist of design deliverables set forth in refs. a. "UFC 4-010-06, Cybersecurity of Facility-Related Control Systems." The CSC-MCX will review all design review submissions prepared by the Designer of Record (government or non-government) for any USACE Military Programs focused design-build and or design-bid-build project.

(4) Review technical requirements for Architect-Engineer and construction contract solicitation packages for the purpose of ensuring appropriate inclusion of FRCS cybersecurity requirements. For design-bid-build projects, review is required for the design statement of work and the construction statement of work. For design-build projects review is required for the design-build statement of work. MCX review to occur as part of technical preparation and review prior to approval/certification by the district Chief of Engineering.

(5) Review FRCS cybersecurity construction submittals requiring Government approval. Review of submittals will consist of deliverables set forth in ref. b. "UFGS 25 05 11, Cybersecurity of Facility-Related Control Systems."