DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
441 G Street, NW
Washington, D.C. 20314-1000

ER 1110-1-8174

CECW-CE

Regulation
No. 1110-1-8174

30 October 2020

Engineering and Design
MILITARY PROGRAMS CONTROL SYSTEM CYBERSECURITY
MANDATORY CENTER OF EXPERTISE (CSC-MCX)

CONTENTS

This Page Intentionally Left Blank

1. Purpose. This regulation sets forth the policies, roles and responsibilities of the U.S. Army Corps of Engineers (USACE) Military Programs Control Systems Cybersecurity Mandatory Center of Expertise (CSC-MCX). It also defines the Mandatory Services which must be requested by, and provided to, USACE districts executing Military Programs projects that include facility-related control systems or low voltage systems.

2. Applicability. This regulation applies to all USACE Commands and to other Department of Defense (DOD) agencies having design and/or construction responsibilities required, or electing, to use CSC-MCX services. The Mandatory Services defined in this regulation apply to all Military Programs projects including but not limited to Military Construction (MILCON), Interagency and International Services (IIS) (i.e. Support for Others), and Sustainment, Restoration, and Modernization (SRM).

3. Distribution. Approved for public release; distribution is unlimited.

4. References.

a. Unified Facilities Criteria (UFC) 4-010-06, 18 Jan 2017, subject: Cybersecurity of Facility-Related Control Systems, with Change 1
https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

b. Unified Facilities Guide Specification (UFGS) 25 05 11, 1 Nov 2017, subject: Cybersecurity for Facility-Related Control Systems
https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11

c. Engineer Regulation (ER) 1110-1-8158, Corps-Wide Centers of Expertise Program
https://www.publications.usace.army.mil/Portals/76/Publications/EngineerRegulations/ER_1110-1-8158.pdf?ver=HE0aLi7qxmM7R46rFQvr4A%3d%3d

d. Department of Defense Instruction (DODI) 8500.01, 14 Mar 2014, Cybersecurity
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf?ver=2019-10-07-112048-860

e. Department of Defense Instruction (DODI) 8510.01, 12 Mar 2014, Risk Management Framework for Department of Defense (DOD) Information Technology (IT)
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

f. Office of the Assistant Chief of Staff for Installation Management (OACSIM), Feb 2017, subject: Army Cybersecurity Strategy for Facility-Related Control Systems

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

h. Army Regulation (AR) 420-1, subject: Army Facilities Management
https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=84190

i. MIL-STD 3007G, Standard Practice Unified Facilities Criteria, Facilities Criteria and Unified Facilities Guide Specifications, 01 NOV 2019
https://www.wbdg.org/ffc/dod/federal-military-specifications-standards/mil-std-3007

5. Records Management (Recordkeeping) Requirements. The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Army Records Retention Schedule—Army (RRS-A). Detailed information for all related record numbers are located in the Army Records Information Management System (ARIMS)/RRS-A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS-A, see Department of the Army (DA) Pamphlet 25-403, Guide to Recordkeeping in the Army.

6. Background. Control systems cybersecurity is an evolving, critical mission requirement for the Army. Director of Army Staff memo of 4 October 2019 directed the Chief of Engineers to develop an overarching program structure for Control Systems that integrates common processes for procurement, configuration, cybersecurity, training, testing and lifecycle management activities across the Army. The Chief of Engineers assigned this responsibility to HQUSACE Military Programs.

a. In collaboration with Army and USACE stakeholders, the Installation Readiness Division (IRD) provides enterprise-wide Control Systems program and policy development, program management, and policy integration. IRD collaborates and communicates with Army organizations involved in Control Systems, manages and facilitates resolution of program issues, and ensures that proper funding is issued to supporting programs when applicable. MIL-STD 3007 identifies the Chief of Engineering and Construction Division as an Engineering Senior Executive Panel member, responsible for development, technical enforcement, equivalencies, and exemptions to Unified Facilities Criteria for the Army.

b. Assuring the confidentiality, availability, and integrity of information and the control systems that support DOD facilities and infrastructure is a critical-path technical requirement to all DOD facility projects. USACE has acknowledged the critical nature of control system cybersecurity in the delivery of stakeholder requirements and therefore, established the Control System Cybersecurity Mandatory Center of Expertise at the U.S. Army Engineering and Support Center, Huntsville to ensure USACE delivers cyber-secure facility-related control systems and other low voltage systems (e.g. nurse call systems) and components to its Military Programs stakeholders.

7. Mission. The CSC-MCX provides highly specialized expertise in facility-related control systems cybersecurity, planning, engineering, design and construction support to USACE activities, the Army, and other DOD and non-DOD federal agencies. The CSC-MCX also provides support to HQUSACE in the creation of design and construction policies, technical guidance, procedures, criteria, specifications, and standards when tasked and funded.

8. Organization. The CSC-MCX organization reports to the USACE Engineering and Support Center, Huntsville Director of Engineering. An organization chart is included in Appendix A.

9. Roles and Responsibilities.

a. Headquarters USACE (HQUSACE). The Chief of Engineering and Construction Division (CECW-CE) is assigned responsibility for the CSC-MCX and will assign an HQUSACE proponent. The Chief of Installation Readiness Division, Military Programs Directorate (CEMP-IRD) will assign a control systems program manager to communicate cybersecurity and other relevant Army policies to the HQUSACE technical elements.

b. HQUSACE Proponent. The HQUSACE proponent will coordinate with the USACE Installation Readiness Division's Control System Program Manager to identify what cybersecurity policies must be implemented and with the USACE Engineering and Construction Cybersecurity Lead and Control System Community of Practice Leader to identify how to implement the policy with specifications and criteria. The Proponent will ensure the CSC-MCX has the latest policy and implementation requirements.

c. USACE Major Subordinate Commands (MSC). Consistent with ER 1110-1-8158, each MSC is responsible for monitoring the activities of their districts and ensuring appropriate use of the CSC-MCX for FRCS cybersecurity planning, engineering, design and construction activities. The MSC is also responsible to ensure any proposed exceptions to the use of CSC-MCX services are coordinated with the CSC-MCX and HQUSACE Proponent. MSC will review any proposed exceptions to the use of CSC-MCX services prior to submitting to HQUSACE (CECW-CE) for consideration.

d. USACE Graphic District. All geographic districts are responsible for engaging the CSC-MCX consistent with this ER and providing funding for execution of CSC-MCX services. MILCON and Non-MILCON (e.g. Sustainment, and Restoration and Modernization (SRM)) projects are executed by the geographic district within their area of responsibility utilizing support from the CSC-MCX consistent with this ER. Each geographic district is responsible for identifying and following any existing MOA's and other agreements. Consistent with 1110-1-8158, districts will include statements in their project documentation, signed by the Chief of Engineering, certifying that the CSC-MCX has been appropriately used in the planning, design, and execution of the project per the support agreement(s) developed by the local district and CSC-MCX. Geographic districts remain responsible for performing the Biddability, Constructability, Operability, Environmental, and Sustainability review.

e. USACE Engineering and Support Center, Huntsville (HNC). HNC will provide the management and technical support to the CSC-MCX that is necessary for the successful execution of the mission and function identified in this regulation. HNC leadership will assure that staffing levels in the CSC-MCX are adequate to handle all tasks assigned in this regulation. Organizational and administrative support such as office space, contracting and computer hardware and software will be provided by HNC. Mission and functions of the CSC-MCX will not be changed without the approval of CECW-CE.

10. Definition of Facility-Related Control System (FRCS).

a. Refer to Reference a. for further description of facility-related control system components.

b. FRCS that fall under the scope of this ER are any systems that control equipment and infrastructure that is part of a building, structure, or linear structure including, but not limited to:

(1) Utility Monitoring Control System, also known as Building Automation System or Energy Monitoring Control System

(2) Building Control System

(3) Electronic Security System

(4) Utility Control System, some of which are also known as Supervisory Control and Data Acquisition Systems

(5) Fire and Life Safety System, also known as Fire Alarm and Fire Suppression System

c. Projects, control systems, and/or control system components which do not fall within the scope of this ER are:

(1) Control Systems funded with Civil Works Appropriations

(2) Control Systems owned by USACE regardless of funding source

11. Mandatory and Optional Services.

a. Determination of Mandatory Services. The intent of mandatory services is to support projects where the control system is sufficiently critical or substantial in size to warrant them. The services indicated as mandatory are applicable to USACE activities within the USACE Military Programs area of responsibility involved with any of the following:

(1) MILCON (including Unspecified Minor Military Construction).

(2) SRM project(s) related to Task Critical and or Defense Critical Asset.

(3) SRM projects which have requirements related to FRCS, and the estimated design and construction cost related to FRCS is greater than $250,000.

(4) IIS projects which have requirements related to FRCS, and the estimated design and construction cost related to FRCS is greater than $250,000.

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

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

b. Mandatory Services. The CSC-MCX will provide the following mandatory services after a receipt of request and appropriate funding:

(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."

c. Optional Services. The CSC-MCX can provide the following voluntary / optional services after receipt of a request, appropriate funding and subject to the availability of CSC-MCX personnel resources.

(1) Any of the services listed above as mandatory services can also be provided as optional services.

(2) Comprehensive system security engineering / cybersecurity consulting services to include but not limited to:

(a) Risk management framework support following DODI 8510.01, Risk Management Framework for Department of Defense Information Technology, and UFC 4-010-06, Cybersecurity of Facility-Related Control Systems (e.g. System Security Plan Development, RMF Artifact Development, etc.).

(b) FRCS Inventories

(c) FRCS cybersecurity compliance assessments

(d) Enterprise Mission Assurance Support Service support

(e) Application of Security Technical Implementation Guides and or Secure Configuration Guides to FRCS

(3) Comprehensive FRCS cybersecurity planning, programming support and in-house design services.

(4) Supporting any on-site quality / performance verification activities, and other acceptance tests.

(5) Supporting as a technical advisor for architect-engineer and or services-based acquisition source selection.

(6) Provide FRCS cybersecurity training.

d. Support to HQUSACE. The CSC-MCX will provide the following support services after receipt of a request and appropriate funding.

(1) Develop and update standards and criteria pertaining to Cybersecurity of Facility-Related Control Systems and other specific criteria and or specifications upon request by HQUSACE. Funding will be provided by HQUSACE Standards and Criteria Program or reimbursable by the requesting agency.

(2) Develop, review and provide subject matter expert input to policy, guidance and other technical and programmatic documents in support of the IRD and the USACE Control System Program.

(3) Represent HQUSACE at select conferences and technical working groups, focusing on FRCS cybersecurity.

(4) Execute special taskings as required and when appropriately funded by HQUSACE.

12. Task Initiation and Procedures. All services are reimbursable except for review of Army Major MILCON DD1391(s) which are centrally funded by HQUSACE. There are no specific exceptions to mandatory use of the CSC-MCX. Requests for exceptions must be fully justified by the USACE activity and submitted to the HQUSACE proponent for approval. To obtain services from the CSC-MCX:

a. Contact the CSC-MCX via email (CSC-MCX@usace.army.mil) and request the mandatory services listed in paragraph 10 a. above. Involve the CSC-MCX as early as possible. The CSC-MCX will provide a cost and estimated time for execution for the service requested along with funding directions i.e. (organization code, resource management point of contact, etc.).

b. Provide design submittals to the CSC-MCX for review. Documentation for review can be provided via a secure file transfer protocol i.e. DoD SAFE, ProjNet, or other secure data transfer applications.

c. The CSC-MCX will utilize USACE standard applications (e.g. ProjNet, Resident Management System) for comment review and back check reviews for design and construction submittals.

d. CSC-MCX attendance at advance planning activities and design charrettes can be requested as on site or through virtual presence. For activities that have significant time zone differences it is highly recommended that on-site participation occurs.

13. Operating and Reporting.

a. HNC will conduct stakeholder service surveys and provided those results to HQUSACE CSC-MCX proponent. Consistent with the requirements of ref c., HNC will support and maintain the CSC-MCX adequate training opportunities for CSC-MCX personnel to maintain state of the art technical proficiency.

b. HQUSACE, with the support of the CSC-MCX, will ensure that information pertaining to the CSC-MCX is kept current and maintained in electronic format on the USACE Technical Excellence Network at https://apps.usace.army.mil/sites/ten/SitePages/Home.aspx.

c. The CSC-MCX will submit an annual report to the HQUSACE proponent. This report will capture funding information, work accomplishments, strategic initiatives, any lessons learned for the prior fiscal year, and the next FY annual operating budget (including salaries, travel, equipment, and training expenses). The report will be submitted to the HQUSACE proponent within 90 days after the end of each fiscal year. The proponent will forward a copy of the report to the USACE Installation Readiness Division's Control System Program Manager to inform on what policy changes may be needed, and to other USACE Divisions and Programs to inform how those policy changes will impact design and construction activities, construction criteria, and other USACE programs and functions.

14. MCX Recertification. As cybersecurity is a rapidly changing and evolving requirement the CSC-MCX will require more frequent recertification to ensure it remains useful and effective. The CSC-MCX will be recertified using the process defined in ER 1110-1-8158 every 2 years unless this conflicts with the timeframe defined in ER 1110-1-8158.

15. Recommendations for FRCS Cybersecurity Improvement. Comments and recommendations concerning this regulation and or the CSC-MCX are welcome. They may be submitted by memorandum to U.S. Army Corps of Engineers CSC-MCX Proponent (CECW-CE), 441 G Street, NW; Washington, DC 20314-1000 or via email to ControlSystemCOPLeader@usace.army.mil with a furnished copy to the Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX), ATTN: CEHNC-EDS-I, P.O. Box 1600, Huntsville, AL 35807-4301 or via email to CSC-MCX@usace.army.mil.

FOR THE COMMANDER:

LLOYD.JOHN.PHILLIP.1021070595 Digitally signed by LLOYD.JOHN.PHILLIP.1021070595 Date: 2021.01.29 15:33:10 -05'00'

1 Appendix
(See Table of Contents)

JOHN P. LLOYD
COL
Chief of Staff

Appendix A
CSC-MCX Organization Chart

CSC-MCX Organizational Chart