



**US Army Corps
of Engineers®**

ENGINEERING AND CONSTRUCTION BULLETIN

No. 2018-11

Issuing Office: CECW-EC

Issued: 09 Aug 18

Expires: 09 Aug 20

SUBJECT: 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

2. **Purpose.** This ECB provides direction and guidance for the mandate to coordinate cybersecurity requirements for all Control Systems within U.S. Army Corps of Engineers (USACE) or projects executed by USACE for external stakeholders.

3. **Applicability**

a. This ECB applies to all control systems designed and constructed by USACE, including but not limited to: supervisory control and data acquisition systems (SCADA), critical infrastructure control systems, electronic security systems (ESS), utility monitoring control systems (UMCS) and fire and life safety systems.

b. This ECB applies to all projects and programs delivering control systems, regardless of whether these control systems are ultimately owned and operated by USACE (USACE asset) or are delivered as a part of an USACE executed project turned over to all stakeholders.

c. This ECB applies to active and future projects whether in design or under construction. It is understood that this will have the potential to impose resource and schedule burdens on projects. However, due to the recent changes in DoD cybersecurity policy and its applicability to control systems, it is imperative to incorporate these critical elements into all USACE execution efforts.

4. **Background**

a. Facilities, Installations, and Civil Works (CW) resources are platforms for mission readiness and critical to the operation and sustainment of our Nation's critical infrastructure. 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 CW, Military Programs (MP), work for others (WFO), Support for Others (SFO), and Environmental Programs. USACE is responsible for both the operation of USACE assets from cradle to grave and for the seamless turnover of constructed facilities to other organizations. In both cases, cybersecurity is essential to the mission of the Army and the defense of the Nation.

c. USACE is evolving its capabilities to support control system cybersecurity requirements across the USACE enterprise by the establishment of two cybersecurity mandatory centers of expertise which support the design and construction mission and the cyber sustainment and operations mission. Both MCXs have been approved and are now mandatory; Engineering Regulations governing them will be released in FY19.

(1) The Critical Infrastructure Cybersecurity Mandatory Center of Expertise (CICS-MCX) coordinates and standardizes cybersecurity methodology, processes and procedures, and system authorization efforts for USACE assets in accordance with DoD and Army requirements. It was established as the national authority over Civil Works control systems across all business

lines and mission areas including national and critical infrastructure and USACE owned and operated control systems under the authority of the USACE Authorizing Official (AO). The CICS-MCX tracks new USACE assets to ensure they are received with appropriate cybersecurity measures in place. The CICS-MCX has multiple geographic locations across the nation and operates under the Command of Southwestern Division (SWD) with its headquarters located within the Little Rock District (SWL) at Table Rock Project.

(2) 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. In order to provide coordination of cybersecurity design and to track accomplishment of USACE Campaign Plan Objective Priority Action Outcomes 1b2.2 and 4b1.3 and provide semi-annual reporting:

(1) For Civil Works Programs projects, and projects resulting in control systems owned by USACE:

(a) Until the engineering regulation (ER) governing the CICS-MCX is released, coordinate cybersecurity design for each system with the CICS-MCX in accordance with the mandatory function list in Attachment (2). CICS-MCX is centrally funded for coordination for these mandatory functions.

(b) After the ER governing the CICS-MCX is released, coordinate cybersecurity design for each system with the CICS-MCX in accordance with the ER.

(c) For each system designed, complete attachment (1) and submit it to the CICS-MCX.

(2) For all Military Programs (military construction (MILCON) and sustainment, restoration, and modernization (SRM)) projects that deliver control systems:

(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 (3) for projects that include control systems and for which one or more of the following apply:

1. Project requires a DD 1391
2. Project exceeds \$7.5 million in total project costs
3. USACE is the primary construction agent.

Costs for the coordination of cybersecurity design is on a reimbursable basis; provide project funding to CSC-MCX for these services.

ECB No. 2018-11

Subject Control System Cybersecurity Coordination Requirement

(b) 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) For each system designed, complete Attachment 1 and submit it to the CSC-MCX.

(3) All other projects (e.g. “work for others”) must continue to implement cybersecurity guidance in project execution, and must coordinate with the appropriate center as described above. There are no specific reporting requirements for these other systems.

(4) 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).

b. 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.

c. Additional coordination and collaboration with the cybersecurity mandatory centers of expertise is always encouraged. In addition to the mandatory services, these centers provide 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.

d. The CICS-MCX point of contact for this action is Phil Copeland, CESWL-OP-X, 501-340-1777, Phillip.L.Copeland@usace.army.mil or DLL-CICS_ICS_CyberSecurity@usace.army.mil.

e. The CSC-MCX point of contact for this action is Daniel Shepard, CEHNC-EDS-I, 256-895-1178, Daniel.A.Shepard@usace.army.mil 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//

LARRY D. McCALLISTER, PhD, PE, PMP, SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers

Encls


Attachment 1 – USACE Cybersecurity Engineering & Construction Checklist

Attachment 2 – CICS-MCX Mandatory Services

Attachment 3 – CSC-MCX Mandatory Services

ATTACHMENT 1: USACE Cybersecurity Engineering & Construction Checklist

This checklist must be submitted to the CICS-MCX or CSC-MCX in electronic format using the Microsoft Excel version of the checklist available upon request from the CICS-MCX, CSC-MCX, or HQUSACE POCs listed in the ECB.

 ECB No. 2018-11, Attachment (1) USACE Cybersecurity Engineering & Construction Checklist					
Project Phase	Required Activities	Deliverable	Status	Date Completed	Additional Comments
Planning					
1	Identify and document all control systems associated with the project	Draft Risk Management Plan (CW) Planning Charrette Validation Form (MP)	<input type="checkbox"/> Completed		
2	Identify and document the System Owner and Authorizing Official for each control system	Draft Risk Management Plan (CW) Planning Charrette Validation Form (MP)	<input type="checkbox"/> Completed		
3	Discuss network connectivity requirements of project control system	Draft Risk Management Plan (CW) Planning Charrette Validation Form (MP)	<input type="checkbox"/> Completed		
4	Determine if there are any existing control system Authorities to Operate (ATO) related to project scope	Draft Risk Management Plan (CW) Planning Charrette Validation Form (MP)	<input type="checkbox"/> Completed		
5	Identify and document any other control system constraints / interdependencies (Privatized Utilities, Existing 3rd Party Financed Energy Contracts, etc.)	Draft Risk Management Plan (CW) Planning Charrette Validation Form (MP)	<input type="checkbox"/> Completed		
6	Include budgetary line item for control system Cybersecurity per system identified within project scope	Draft Risk Management Plan (CW) Completed 1391 (MP)	<input type="checkbox"/> Completed		
7	Geographic District inform and provide USACE Cybersecurity CX's (CICS-MCX Civil Works & CSC-MCX Military Programs) project scope.	Draft Risk Management Plan (CW) Completed 1391 (MP)	<input type="checkbox"/> Completed		
Design (Refer to UFC 4-010-06 "Cybersecurity of Facility Related Control Systems with Change 1")					
1	Ensure UFC 4-010-06 Cybersecurity requirements are in A/E SOW & include cybersecurity in contract evaluation (for AE designs) -OR- that the designer has reviewed and understands UFC 4-010-06 requirements (for in-house design)	Design SOW/PWS or Designer Review	<input type="checkbox"/> Completed		
2	Ensure a single submittal indicating the Confidentiality (C), Integrity (I) and Availability (A) impact level for each control system (s) within the project scope is delivered by the designer of record	Design Submittal (Basis of Design)	<input type="checkbox"/> Completed		
3	Ensure a listing of the security controls are generated and delivered by the designer of record. Security Controls should correspond to the system(s) determined (C-I-A) impact level.	Design Submittal (Basis of Design)	<input type="checkbox"/> Completed		
4	Ensure the designer of record generates and delivers a list of corresponding control correlation identifiers (CCIs) which are derived from the selected security controls	Design Submittal (10-15% Parametric Design)	<input type="checkbox"/> Completed		
5	Ensure the designer of record categorizes all CCIs and address all identified as "Designer" specific.	Design Submittal (35% Design Submittal)	<input type="checkbox"/> Completed		
6	Ensure designer of record incorporates minimum cybersecurity design requirements IAW Chapter 4 UFC 4-010-06	Design Submittal (60% Design Submittal)	<input type="checkbox"/> Completed		
7	Ensure designer of record incorporates any required changes from previous design submittal as a pre-final design	Design Submittal (90% Design Submittal)	<input type="checkbox"/> Completed		
8	Ensure designer of record submits final and complete design	Design Submittal (100% Design Submittal)	<input type="checkbox"/> Completed		
9	Post Design Effort inform and report to USACE Cybersecurity CX's (CICS-MCX Civil Works & CSC-MCX Military Programs)	Email	<input type="checkbox"/> Completed		



ECB No. 2018-11, Attachment (1)

USACE Cybersecurity Engineering & Construction Checklist

Project Phase	Required Activities	Deliverable	Status	Date Completed	Additional Comments
Construction (Refer to UFGS 25-05-11 "Cybersecurity for Facility Related Control Systems")					
1	Ensure Construction RFP includes Unified Facilities Guide Specification (UFGS) 25-05-11 Cybersecurity for Facility Related Control Systems in SOW/PWS specifications section	Construction SOW/PWS	<input type="checkbox"/> Completed		
2	Ensure a cross reference to other functional UFGS conducted and incorporated into the Construction RFP	Construction SOW/PWS	<input type="checkbox"/> Completed		
3	Ensure all Construction Submittals identified in section 1.6 of UFGS 25-05-11 are delivered and proper Government acceptance is documented	Construction Submittal	<input type="checkbox"/> Completed		
4	Ensure coordination with Facility Owner, System(s) Owner for scheduling of Security Control Assessor-Validator (SCA-V) Assessment (Coordination of Master Schedule in line with Systems Commissioning Efforts should occur at this time)	Schedule Confirmation	<input type="checkbox"/> Completed		
5	Confirm System Owner has submitted Risk Management Framework (RMF) Authorization Package to Authorization Official (AO) via eMASS	Confirmation	<input type="checkbox"/> Completed		
6	Confirm RMF Authority to Operate (ATO) for all systems is granted prior to facility acceptance BOD i.e. DD1354	Confirmation	<input type="checkbox"/> Completed		
7	Inform and report to USACE Cybersecurity CX's (CICS-MCX Civil Works & CSC-MCX Military Programs)	Email	<input type="checkbox"/> Completed		
Post Construction / Project Closeout					
1	Provide All Closeout Documentation to Facility Owner and System Owner	User Manuals, Warranty Documentation, Updated Redline Drawings & As-Builts	<input type="checkbox"/> Completed		
2	Inform and report to USACE Cybersecurity CX's (CICS-MCX Civil Works & CSC-MCX Military Programs)	Email	<input type="checkbox"/> Completed		

ATTACHMENT 2: CICS-MCX Mandatory Services

For each project required by the ECB to coordinate with the CICS-MCX, coordinate the following with the CICS-MCX:

- a. Coordinate CSC-MCS performance of site cybersecurity surveys, cyber-risk assessments and physical security assessments of cyber assets
- b. Coordinate with the CSC-MCX to provide guidance to ISO regarding the appointment of cybersecurity personnel
- c. Provide designs and specifications to CICS-MCX for review at 30% - 60% - 90% and final (prior to release for advertising)
- d. Provide cybersecurity-related project submittals to CICS-MCX for review
- e. Coordinate response to vendor-requested clarifications on cybersecurity requirements with the CSC-MCX
- f. Provide required vendor documentation and system security scans to CICS-MCX for review prior to installation for determining Interim Secure State (ISS)
- g. Coordinate ISSM-R participation in pre-delivery, performance verification, and other acceptance tests (e.g., Factory Acceptance Testing) with the CICS-MCX Director
- h. Coordinate final security control validation with the CICS-MCX, where the CICS-MCX will serve as the Security Control Assessor - Organization (SCA-O) in order to obtain an Authority to Operate (ATO) for the system.

ATTACHMENT 3: CSC-MCX Mandatory Services

For each project required by the ECB to coordinate with the CSC-MCX, coordinate with the CSC-MCX as follows:

1. Planning Phase

- 1.1. For 1391 development, provide pre-design requirements and planning documents to CSC-MCX for review. CSC-MCX will provide input to establish Rough Order of Magnitude (ROM) for 1391
- 1.2. Provide 1391 to the CSC-MCX for review

2. Contracting Services

- 2.1. Coordinate contract source selection with CSC-MCX. CSC-MCS will provide input and advice to support acquisition strategy selection

3. Design Phase

- 3.1. Provide Designer of Record design scope of work (SOW) to CSC-MCX for review for each phase of SOW development (e.g., draft, draft final, final)
- 3.2. Provide design documents to CSC-MCX for review at the following design stages (or at equivalent design stages should these levels not be used)
 - 3.2.1. 30% design
 - 3.2.2. 60% design
 - 3.2.3. 90% design

4. Construction Phase

- 4.1. Provide pre-testing review materials to the CSC-MCX and coordinate attendance of testing by the CSC-MCX.