

CECW-CO

Regulation
No. 25-1-113

31 January 2019

Engineering and Design
USACE CRITICAL INFRASTRUCTURE CYBERSECURITY
MANDATORY CENTER OF EXPERTISE

1. Purpose. This regulation establishes policies, roles, and responsibilities for the U.S Army Corps of Engineers (USACE) Critical Infrastructure Cybersecurity Mandatory Center of Expertise (UCIC-MCX) to assure that new and existing projects and facilities with control systems that are owned and operated by USACE are secured and authorized according to applicable Department of Defense and Army regulations. The center serves to protect control systems and enable the systems to obtain an Authority to Operate (ATO). It also establishes the mandatory functions of the UCIC-MCX that major subordinate commands (MSCs) will utilize to advance the security of USACE control systems. This regulation officially renames the Critical Infrastructure Cybersecurity Center of Expertise (CICSCX) to the UCIC-MCX.

2. Applicability. This regulation applies to all USACE MSC's, districts, centers, laboratories, and Field Operating Activities (FOAs) that: a) own and operate control systems across all business lines and mission areas, or b) design Civil Works control systems, or c) design any other control systems that will be owned and operated by USACE.

This regulation applies to the cybersecurity of control systems as defined in Appendix D of this regulation and categorized as one of the following:

a. National Critical Infrastructure Control Systems which include but are not limited to:

- (1) Hydropower Control Systems
- (2) Water Management Control Systems
- (3) Navigation Control Systems
- (4) Flood Risk Management Control Systems
- (5) Dam Safety Control Systems
- (6) Water Supply Control Systems
- (7) Environmental Stewardship Control System
- (8) Marine Traffic Control System
- (9) Auxiliary Hydropower Control System

b. Other Control Systems which include but are not limited to:

- (1) Building Control System
- (2) Electronic Security System
- (3) Fire and Life Safety
- (4) Traffic Control Systems
- (5) Energy Monitoring Control System
- (6) Utility Monitoring Control System
- (7) Utility Control System

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

4. References. This regulation will adhere to the most current version of the listed references and all successor documents.

a. Title 42 United States Code, Chapter 68, Subchapter IV-B, Sec. 5195c - Critical Infrastructures Protection (Critical Infrastructures Protection Act of 2001); <https://www.gpo.gov>

b. Public Law 107-296 - NOV. 25, 2002; Homeland Security Act of 2002; <https://www.gpo.gov>

c. Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience, February 12, 2013; <https://www.whitehouse.gov>

d. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 12, 2013; <https://www.whitehouse.gov>

e. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 11 May 2017; <https://www.whitehouse.gov>

f. Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, 14 March 2014; <http://www.dtic.mil/whs/directives/>

g. Department of Defense Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014; <http://www.dtic.mil/whs/directives/>

h. Department of Defense Manual, DoD 8570.01-M, Information Assurance Workforce Improvement Program, December 19, 2005 incorporating Change 4, November 10, 2015; <http://www.dtic.mil/whs/directives/>

i. Army Regulation (AR) 25-2, Information Assurance; <https://armypubs.army.mil>

j. Engineer Regulation (ER) 1110-1-8158, Corps-Wide Centers of Expertise Program; www.publications.usace.army.mil

k. US Army Network Enterprise Technology Command, Stand-Alone Information System and Closed Restricted Network Assessment and Authorization Operational Tactics, Techniques, and Procedures, Version 1, 27 June 2016; <https://netcom.army.mil/>

l. National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations, December 2018

m. NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security, May 2015; <https://csrc.nist.gov/publications/>

n. Appointment Memorandum 16-01, Appointment of the Civil Works Control Systems National Information System Security Manager (ISSM-N), and the USACE Control System Cybersecurity Center of Expertise (CICSCX)

5. Background. Protecting control systems to securely function in an ever-changing cyber threat landscape and designing systems with security measures that can be safely deployed to control and monitor critical infrastructure is a highly specialized endeavor and requires significant expertise beyond that of typical control system engineers. Staying abreast of the changing threats and discovered vulnerabilities in control system components requires diligence and focus. USACE recognized the critical nature of control system cybersecurity and appointed a National Information Assurance Manager (IAM) for all Civil Works control systems in January, 2014. That appointment was updated in December 2016 through reference (n), which designates national authority for control system cybersecurity to the CICSCX across all Civil Works business lines and mission areas.

6. Policy. The expertise of the UCIC-MCX will be utilized to secure USACE owned and operated control systems throughout the system development life cycle ensuring that they are designed and operated at an acceptable cyber risk level according to the most current DoD, Army, and USACE regulations.

7. Roles and Responsibilities.

a. Headquarters (HQ) USACE. HQUSACE will appoint a proponent for the UCIC-MCX according to ER 1110-1-8158. The HQUSACE Proponent will appoint a HQ employee as the Program Manager (PgM) of the UCIC-MCX per ER 1110-1-8158. The HQ Proponent or their representative along with the PgM will ensure the Center is completing its mission according to this regulation.

b. Supporting MSC Command. According to ER 1110-1-8158, the Supporting MSC Command is the Southwestern Division and will support the UCIC-MCX by providing quality assurance/quality control of services delivered to using commands. The Supporting MSC Command is responsible for providing sufficient training opportunities to enable UCIC-MCX personnel to maintain state-of-the-art proficiency in their assigned position.

c. Using Commands. Using commands (i.e., USACE MSCs, districts, centers, laboratories, and FOAs) will coordinate with and use the UCIC-MCX mandatory functions as detailed in Appendix A and B of this regulation. Using commands are responsible for completing and maintaining a comprehensive inventory of all USACE-owned control systems in their area of responsibility. Inventory data will be provided to the UCIC-MCX annually, when significant changes in inventory data occurs, or as requested by the UCIC-MCX. Using commands are also responsible for appointing personnel to cybersecurity roles (also known as Information Assurance (IA)) for every control system according to references (f) and (g). Appointed cybersecurity personnel must be qualified according to references (h) and (i). Cybersecurity (IA) roles are further described in Appendix D of this regulation. Using commands will provide the UCIC-MCX the physical and logical (system/network/computer) access required for the Center to perform the duties outlined in Appendix A and B of this regulation. Using commands will use UCIC-MCX developed policy and procedures documents for the assessment and authorization process requirements.

d. UCIC-MCX. The Center is staffed with subject matter experts (SMEs) experienced in securing control systems for the safe and effective operation and maintenance of critical infrastructure and USACE facilities. The Center SMEs will maintain state-of-the-art expertise in control systems and cybersecurity solutions and trends. The Center will maintain expertise in all DoD, Army, and USACE regulations pertaining to control system cybersecurity. The functions of the UCIC-MCX are detailed in Appendix A and B of this regulation.

8. Function Statement. The UCIC-MCX will identify, assess, and address control system cybersecurity matters according to DoD and Army regulations by executing the functions outlined in Appendix A and B of this regulation. Although the UCIC-MCX provides design support through supplying and reviewing cybersecurity requirements for new and existing control systems that will be or are owned and operated by USACE, it does not function as a design and engineering center for control systems.

9. Operating and Reporting.

a. The HQUSACE proponent of the UCIC-MCX is HQUSACE Chief, Operations and Regulatory Division. As such, this regulation is fulfilling the requirements of ER 1110-1-8158.

b. The appointed HQ PgM for the UCIC-MCX is the Deputy Chief, Operations and Regulatory Division.

c. The UCIC-MCX Director is appointed the ISSM-N by the Director of Civil Works. The ISSM-N is formally appointed as an IAM III per reference (h) of this regulation and is appointed the Security Control Assessor – Organization (SCA-O) for USACE control systems by the USACE Authorizing Official (AO).

d. The UCIC-MCX Director reports to the Deputy Chief, Operations and Regulatory Division at Headquarters, USACE.

e. The Center has multiple geographic locations across the nation and operates under the Command of Southwestern Division with its headquarters located within the Little Rock District (SWL) in Branson, Missouri.

f. According to ER 1110-1-8158, HQUSACE PgM will conduct customer service surveys and provide those results to the HQUSACE proponent.

g. HQUSACE, with the support of the UCIC-MCX, will ensure that information pertaining to cybersecurity requirements, policies, cybersecurity implementation technical guidance, etc., is kept current and maintained in electronic format on a dedicated UCIC-MCX knowledge management site. The site will be accessible by all USACE employees.

h. The UCIC-MCX will submit an annual report to HQUSACE. This report will capture funding information, work accomplishments, strategic initiatives, and lessons learned for the prior fiscal year. The report will be submitted to HQUSACE within 90 days after the end of each fiscal year.

10. Funding. All functions of the UCIC-MCX, as defined in Appendix A and B, related to USACE owned and operated Civil Works control systems are centrally funded with Civil Works Operation and Maintenance (CW O&M) funds as a Remaining Item in the President's Budget. All functions of the UCIC-MCX, as defined in Appendix A and B, related to USACE owned and operated, non-Civil Works control systems are centrally funded by Operations Maintenance Army (OMA) funds from the USACE Chief Information Officer. UCIC-MCX personnel and overhead costs are funded proportionately from CW O&M funds and OMA funds based on the anticipated level of support to be provided to USACE owned and operated Civil Works and non-Civil Works control systems. The UCIC-MCX will recalibrate this proportional split annually to ensure that it accurately reflects the services provided to Civil Works and non-Civil Works control systems. Additional services to using commands as defined in Appendix C will be executed by mutual agreement on a fully cost reimbursable basis. The UCIC-MCX is required to strictly adhere to these funding requirements to avoid fiscal law violations.

11. Agency Representation. For USACE-owned and -operated control systems, the UCIC-MCX is the authorized USACE cybersecurity representative for collaboration on cybersecurity with entities external to USACE. The UCIC-MCX communicates the strategic direction and execution of cyber policy and guidance for control systems on behalf of USACE organizations. External entities to include, but are not limited to, The Office of Secretary of Defense (OSD), Department of Homeland Security, Department of Army, Army Cyber Command, NETCOM, Bureau of Reclamation, private industry, etc. Any USACE communications with these and other entities will be coordinated through the UCIC-MCX.

12. Conflict Resolution. Conflicts or differences will be resolved between the UCIC-MCX and the using command at the lowest level necessary. If a conflict or difference develops that cannot be resolved by mutual agreement between the parties involved, it will then be elevated to the Command's senior leadership for resolution. Finally, because the UCIC-MCX is a Corps-wide asset, HQUSACE may be requested by either the UCIC-MCX or the


using command to resolve the conflict or difference. Final resolution as determined by senior leadership and HQUSACE will be posted on the UCIC-MCX knowledge management site.

13. Exceptions. A request for an exception to the requirements of the regulation will be fully justified and submitted through the MSC Command to the HQUSACE proponent for approval according to ER 1110-1-8158.

14. Recertification. The UCIC-MCX will be recertified as an MCX every 5 years according to the appropriate requirements of ER 1110-1-8158. Six months before its recertification date, the UCIC-MCX will provide the HQUSACE proponent with a draft evaluation of the continuing need for the MCX against the performance statements.

FOR THE COMMANDER:

3 Appendices
Appendix A MCX Mission and
Function Statements
Appendix B Mandatory Function Workflows
Appendix C Reimbursable Services Glossary



RAFAEL F. PAZOS
COL, EN
Chief of Staff

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A
MCX Mission and Function Statements

A-1. Mission. The USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise (UCIC-MCX) has national authority over USACE owned and operated control system cybersecurity. The UCIC-MCX provides national level oversight and guidance for all USACE owned and operated control system cybersecurity by directing, coordinating, and standardizing cybersecurity methodology, processes and procedures, and system authorization efforts according to DoD and Army requirements to assure that control systems operate at an acceptable level of cyber risk. The UCIC-MCX has cybersecurity purview over USACE MSC, Districts, Centers, Laboratories, and FOA across Civil Works business lines and mission areas and all other USACE owned and operated control systems that fall under the authority of the USACE AO.

The UCIC-MCX Director is appointed the ISSM-N by the Director of Civil Works. The ISSM-N is formally appointed as an IAM III per reference (h) of this regulation and is appointed the SCA – Organization (SCA-O) for USACE control systems by the USACE AO. The UCIC-MCX is located in Branson, Missouri within the Little Rock District.

A-2. Functions. The UCIC-MCX will identify, assess, and address control system cybersecurity matters according to DoD and Army regulations by executing the functions outlined in this statement. Although the UCIC-MCX provides design support through supplying and reviewing cybersecurity requirements for new and existing control systems that will be or are owned and operated by USACE, it does not function as a design and engineering center for control systems. The UCIC-MCX will:

a. Provide national level oversight and guidance for USACE owned and operated control system cybersecurity activities. The UCIC-MCX will:

(1) Maintain a comprehensive and current inventory of control systems owned and operated by USACE. This inventory will directly support multiple MCX functions to include, but is not limited to, issuing vulnerability alerts to system owners;

(2) Manage and direct the implementation of the control system risk management strategy to ensure control systems are logically and physically secure;

(3) Assist Information System Owners (ISO's) with control system component and cyber asset identification and determining the criticality of component and cyber assets;

(4) Actively collaborate with Engineering & Construction (E&C) in regards to control system cybersecurity criteria;

(5) Conduct control system cybersecurity assessments using current DoD cybersecurity requirements to develop remediating and mitigating strategies for ISO's to ensure control systems operate at an acceptable level of risk as determined by the AO;

(6) Direct cybersecurity compliance efforts through MSC Command channels when necessary;

(7) Develop, and provide oversight for, implementation procedures, plans, guidance, and instructions (e.g., standard operating procedures, Tactics, Techniques, & Procedures (TTP's) etc.) for ensuring compliance to new and existing policies relating to control system cybersecurity;

(8) Interpret DoD and Army policy to provide guidance and procedures for control systems in order to obtain an ATO and continually operate at an acceptable level of risk;

(9) Originate official cybersecurity documents for signature by senior leadership. Documents to include, but not limited to, policy statements, memorandums, execution, and posture of cybersecurity related to controls systems;

(10) Represent USACE control system cybersecurity during collaboration with entities internal or external to USACE in order to communicate the technical/USACE execution of cybersecurity policy and guidance. External entities to include, but are not limited to OSD, Department of Homeland Security, Department of Army, Army Cyber Command, NETCOM, Bureau of Reclamation, private industry, etc.;

(11) Coordinate with any agency/organization conducting a cyber-assessment on control systems that does not directly support the system owner's efforts to obtain an ATO, and direct activities to ensure the assessment will not negatively impact the operational capability of the control system;

(12) Standardize cyber incident response procedures for control systems according to applicable DoD and Army policy;

(13) Be first point of contact of any cyber event or incident on a control system and coordinate local incident response activity with appropriate entities;

(14) Appoint Regional Information System Security Managers (ISSM-R) as the first point of contact for using commands' Information System Security Managers (ISSM's) for all USACE owned and operated control system cybersecurity activity, issues, concerns, and cyber events;

(15) Provide qualified Information System Security Engineer and Information Security Architect (ISA), according to reference (h) of this document, to review control system cybersecurity design for using commands that do not have these qualified personnel in place;

(16) Provide oversight of physical security of control systems in coordination with the using command ISSM and physical security personnel;

(17) Liaison to the USACE Cybersecurity Program Manager Office;

(18) Assist Reliability Compliance Program Managers in coordinating the RMF with North American Electric Reliability Compliance Critical Infrastructure Protection compliance;

(19) Actively participate on technical governmental working groups associated with control systems to include, but not limited to, DoD, Army, Bureau of Reclamation, Department of Homeland Security, and the private sector as authorized by controlling guidance, in cooperation with other USACE entities.

b. Manage system assessment and authorization activities as defined in references (f), (g), and (l) for USACE owned and operated control systems. The UCIC-MCX will:

(1) Coordinate with ISO's for cybersecurity evaluation and categorization decisions of systems currently in development or in operation to include developing a System Security Plan (SSP);

(2) Provide project E&C and ISO's with control system cybersecurity requirements, coordinate with the Project Delivery Team (PDT) to review technical specifications (cyber), respond to vendor-requested clarifications on cybersecurity requirements, and participate in the design submittal review to ensure cybersecurity requirements are addressed for any control system acquisition that falls under the authority of the USACE AO;

(3) Assist ISO's with implementing security controls and documenting RMF (or current DoD authorization vehicle) security control compliance;

(4) Provide guidance and support for implementing the Enterprise Mission Assurance System Support (eMASS) database (or DoD mandated database) for RMF activities;

(5) Engage in all SCA – Validator assessment efforts for control systems, and provide SCA-O assessments when applicable according to reference (m) of this document;

(6) Assist ISO's with the mitigation and remediation of vulnerabilities listed on the system's Plan of Action and Milestones (POA&M);

(7) Assist ISO's in generating the ATO request package;

(8) Provide oversight and guidance on continuous monitoring strategies of control systems;

(9) Validate control system cybersecurity posture remains consistent with the system ATO by engaging in the mandated Federal Information Security Modernization Act of 2014 annual review.

c. Monitor and report on USACE owned and operated control system status. The UCIC-MCX will:

(1) Monitor and report the authorization cycle for control systems;

(2) Respond to requests for cybersecurity status of control systems;

(3) Prepare and present required upper level command briefs;

(4) Monitor control system progress on remediation or mitigation activities based on findings from DoD Inspector General and/or Army Inspector General audits and report progress as required.

d. Integrate physical security practices with cybersecurity requirements in new and existing USACE owned and operated control systems. The UCIC-MCX will:

(1) Issue guidance on control system hardening and configuration for control system components (e.g., workstations, servers, programmable logic controllers, etc.) and provide oversight to using commands addressing control system vulnerabilities, ensuring systems operate at an acceptable level of risk. Support and collaborate with using commands that have system hardening expertise and provide hands-on support when requested by projects that do not have this expertise;

(2) Issue guidance on control system hardening and configuration of network devices (e.g., firewall, routers, switches, etc.) and provide oversight to using commands addressing network device vulnerabilities, ensuring systems operate at an acceptable level of risk. Support and collaborate with using commands that have network device configuration expertise and provide hands-on support when requested by projects that do not have this expertise;

(3) The National Supervisory Control and Data Acquisition (SCADA) Test Lab, located at the UCIC-MCX facility, will develop test systems with similar configuration settings to those found at USACE sites in order to assist with evaluating security patch, software update, and security configuration impacts on control systems prior to deployment on the live production system for using commands that do not have this expertise or capability. This will not limit established Centers with cybersecurity expertise from research and development for control system cybersecurity;

(4) Test and evaluate new and existing technologies for their viability and practicality for improving the cybersecurity posture of control systems across USACE;

(5) Oversee and chair working group to issue standards to enhance the physical protection of control systems;

(6) Collaborate with using command physical security personnel concerning all physical security assessments or inspections being conducted on facilities containing USACE owned and operated control systems. The UCIC-MCX Physical Security Specialist Cyber will coordinate travel to the site for the assessment/inspection with the using command physical security personnel if deemed necessary;

(7) Issue the physical security requirements that are necessary to obtain an ATO for USACE owned and operated control systems.

e. Educate the USACE control system workforce. The UCIC-MCX will:

(1) Execute multi-level training on USACE control system cybersecurity to include but not limited to the USACE control system risk management strategy, RMF implementation, eMASS responsibilities, etc.;

(2) Execute security engineering training to equip using command personnel with the tools and capabilities necessary to secure their control systems;

(3) Assist using commands with facilitating cybersecurity certification (formerly known as Information Assurance (IA)) for officially appointed cybersecurity roles as required by DoD and the Army;

(4) Share information with USACE internal stakeholders regarding cybersecurity threats, security trends, and best practices for control system cybersecurity via appropriate communication means for the type of information being shared;

(5) Provide access to the National SCADA Test Lab to Army and USACE entities for the purpose of education, training, and exercises on control systems and cybersecurity solutions when requested and available.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix B Mandatory Function Workflows

B-1. The following provides supporting instruction for the mandatory functions described in Appendix A Section A-2.b(2):

- a. Perform site cybersecurity surveys and physical security assessments of cyber assets;
- b. Provide guidance to ISO regarding the appointment of cybersecurity personnel as described in Section 7.c of the ER and further defined in Appendix D of this regulation;
- c. Conduct a cyber-risk assessment utilizing a standardized tool;
- d. Provide ISO's and PDT with documentation defining current control system cybersecurity requirements;
- e. Coordinate with the PDT to review and approve technical specifications (cyber) at 30% - 60% - 90% and final prior to release for advertising to ensure cybersecurity requirements are addressed according to DoD and Army regulations. If applicable, participate in the Bid-ability, Constructability, Operability, Environmental, and Sustainability review. Participate in Source Selection Board (cyber) as deemed necessary by the UCIC-MCX Director;
- f. Respond to vendor-requested clarifications on cybersecurity requirements prior to contract award;
- g. Participate in and approve vendor (cyber) design submittal reviews;
- h. Review required vendor documentation and system security scans prior to installation for determining Interim Secure State (ISS) as defined in Appendix D;
- i. The ISSM-R will participate in pre-delivery, performance verification, and other acceptance tests (e.g., Factory Acceptance Testing) as deemed necessary by the UCIC-MCX Director;
- j. Perform final security control validation duties as the SCA-O when applicable in order to obtain an ATO for the system.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix C
Reimbursable Services

C-1. The UCIC-MCX is available to perform the following services as requested for MSCs, Districts, Centers, Laboratories, and FOAs on a fully cost reimbursable basis:

a. Perform secure configurations on information technology (IT) and operational technology (OT) assets of control systems and data acquisition systems to meet cybersecurity requirements (i.e. hands-on system securing services);

b. Develop system specific diagrams, drawings, baselines, and/or other system documentation necessary to meet cybersecurity requirements with the approval and oversight of the Center's director.

C-2. The UCIC-MCX services as defined in this ER are available to be provided to federal, state and local governmental agencies when consistent with USACE authorities governing support for others, and with the approval and oversight of HQUSACE.

THIS PAGE INTENTIONALLY LEFT BLANK

Glossary Terms

D-1. Cybersecurity (Information Assurance (IA)) Roles. At a minimum, each ISO will appoint the following two personnel for the cybersecurity of each control system. A description of the following roles, responsibilities, and qualifications can be found in reference (h) and succeeding revisions.

- a. IA Manager I (IAM I), known as ISSM under the RMF;
- b. IA Technical I or II (IAT I or IAT II), referred to as System Administrator under RMF.

D-2. Control System. A control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve a specific physical objective in real or near-real time (e.g., moving a tainter gate or starting a pump or generator). This includes protective systems (e.g., generator relays, transformer relays, etc.) and data acquisition systems that support critical infrastructure missions (e.g., dam safety, water data, etc.). A control system can operate as a stand-alone isolated system, as a closed restricted network across multiple geographic locations, or as a connected system:

- a. Stand-alone Isolated System: A control system that operates in a single geographic location and on a completely isolated, private network;
- b. Closed Restricted Network (CRN): A control system that operates across multiple geographic locations using a virtual private network (VPN) across communication lines with encryption;
- c. Connected System: A control system that has a logical interconnection with an external network.

Further control system definitions can be found in reference (k), (l), and (m).

D-3. Interim Secure State (ISS). ISS is achieved when a control system's risk is known and the system has been verified as being technically and physically secured to an acceptable risk tolerance, but it does not have all documentation and/or administrative requirements met for obtaining an ATO:

- a. Used to verify that a new control system installation, or a system going through a major upgrade, is implementing critical security controls during the installation phase and meets a specific cybersecurity standard prior to the government taking ownership. This standard is specified in the USACE Interim Secure State for Control Systems TTP;
- b. Used to verify that an existing control system is operating at an acceptable state of cybersecurity.

THIS PAGE INTENTIONALLY LEFT BLANK