US Army Corps of Engineers®

ENGINEERING AND CONSTRUCTION BULLETIN

No. 2015-14 **Issuing Office:** CECW-CE **Issued:** 13 Aug 15 **Expires:** 13 Aug 17

SUBJECT: Integrating Cybersecurity Requirements

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. Dept. 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

2. **Purpose.** This ECB provides direction and guidance to support the implementation of cybersecurity requirements into all applicable projects executed by the U.S. Army Corps of Engineers (USACE).

3. **Applicability.** This ECB applies to all projects that include facility related Platform Information Technology (PIT) systems, regardless of acquisition method, funding source, or location (CONUS/OCONUS). These PIT systems include but are not limited to Industrial Control Systems (ICS), Utility Monitoring and Control Systems (UMCS), Electronic Security Systems (ESS), Building Automation Systems (BAS), Supervisory Control and Data Acquisition (SCADA) systems, and similar control systems.

4. **Background.**

a. Recent DoD and Department of the Army (DA) policy changes pertaining to cybersecurity and the recent targeted cyber attacks in the private sector conducted by nation-state cyber criminals have increased the sensitivity to the vulnerabilities and risks associated with automated process and facility control systems referred to in reference (c) as PIT systems, which are frequently included in projects executed by the USACE.

b. Consistent with industry, most DoD PIT systems were built on open architectures with very little thought to cybersecurity. Also, most PIT systems are built on a long sustainment life cycle design (25-30 years) in comparison to traditional IT communication network equipment i.e. desktop computers, laptops, and network switches and routers which have an expected life cycle of 2-5 years. As such, the components and networks of these PIT systems are largely legacy in nature and not immediately suitable to current software and vulnerability mitigation procedures used on traditional IT communication networks and due to the specialized purpose of their application, PIT systems require uniquely tailored security control sets and control validation procedures.

c. In conjunction with the tri-services, USACE ICS Cybersecurity Technical Center of Expertise (TCX) is developing a Unified Facilities Criteria (UFC) that will address cybersecurity requirements for PIT systems. This UFC is anticipated to be published in FY16. USACE is also planning to develop a cybersecurity Unified Facilities Guide Specification (UFGS) in FY16 that will document all execution requirements and contract submittals.

d. Reference (d) requires all information systems and PIT systems to be categorized in accordance with reference (f); a set of security controls implemented from references (f) and (g); use of assessment procedures from reference (g); and authorization by an Authorizing Official (AO), formally referred to as the Designated Approving Authority (DAA), to operate the system based on achieving and maintaining an acceptable risk posture.

5. **Guidance.** It is highly recommended that cybersecurity design and construction requirements for PIT systems be coordinated with the USACE ICS CybersecurityTechnical Center of Expertise (TCX).

6. **Directive.** All PIT included in projects that are delivered by USACE must be planned, designed, acquired, executed and maintained in accordance with references (c) and (d), and as required by individual service implementation policy. Comply with the following:

a. Planning Phase: During the project planning phase, coordinate with the installation network service provider and PIT system owner to identify responsibilities of each organization (such as Network Enterprise Center (NEC), Directorate of Information Management (DOIM), facility owner, system operator, designer, construction contractor, and USACE) and define implementation requirements (PIT vs. non-PIT requirements). Ensure that all planning estimates identify costs for cybersecurity implementation.

b. Design Phase: Ensure the Scope of Work (SOW) for the project designer(s) includes the appropriate cybersecurity requirements defined in the planning phase. During the design phase, the designer(s) must continue to coordinate with all responsible organizations and should develop an initial inventory and system categorization. Ensure the final design documents identify the cybersecurity installation contract/construction contract submittal requirements and acquisition language to complete a final inventory and system categorization, control plans, authorization to operate the system, and authorization to connect to the network as appropriate.

c. System Acquisition, Installation and Construction Phase: Ensure that the contract includes compliance with references (c) and (d), and with individual service implementation policy. As the Army implementation of references (c) and (d) is still in development, it is very important to closely coordinate with the installation network service provider and system owner.

7. **Update.** There are no policy document updates required prior the expiration of this ECB.

8. **Point of Contact:** HQUSACE POC for this ECB is Ms. Elaine Wales, CECW-CE, (256) 895-1732.

//S//
STACEY HIRATA, P.E., SES
Chief, Installation Support Division
Directorate of Military Programs

//S//
JAMES C. DALTON, P.E., SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers