



Cybersecurity Systems Program

Program Manager 256-895-5242

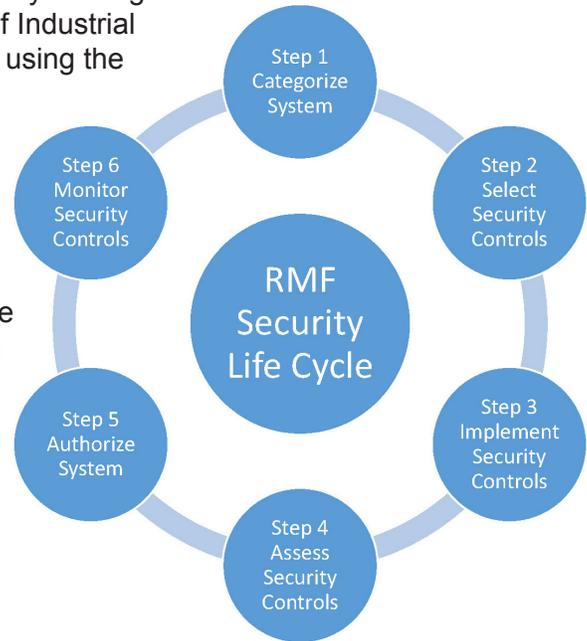
U.S. ARMY CORPS OF ENGINEERS

BUILDING STRONG®

The Engineering and Support Center, Huntsville provides quality oversight for the management of cybersecurity system accreditations of Industrial Control Systems (ICS) for the Department of Defense (DOD) using the Risk Management Framework (RMF) requirements. The Cybersecurity (CS) Program manages cybersecurity projects from inception to completion.

The cybersecurity requirement has been mandated for all DOD per the RMF standards in accordance with the DOD Instructions 8500.01 "Cybersecurity" and 8510.01 "RMF for DOD IT" both updated and released in March 2014. Huntsville Center's CS Program manages these projects from inception to completion. Replacing the DOD Information Assurance Certification and Accreditation Process (DIACAP), RMF comprises six steps:

1. Categorization of information systems
2. Selection of security controls
3. Implementation of security controls
4. Assessment of security controls
5. Authorization of information systems
6. Monitoring of security controls



One of the major differences between DIACAP and the RMF process is that RMF now incorporates continuous monitoring and Authority Termination Dates (ATD) (date of expiration) that can be within any range of up to a three-year period. Any Authority To Operate (ATO) can be extended by the authorizing official upon satisfactory continuous monitoring by the system owners.

Cybersecurity Systems Project Delivery Team

The CS Program works directly with the ICS Cybersecurity Technical Center of Expertise (TCX), also located within Huntsville Center, to Assess and Authorize (A&A) industrial control systems for various DOD customers. ICS can include, but are not limited to, Utility Monitoring and Control Systems (UMCS), Electronic Security Systems (ESS), Building Automation Systems, Supervisory Control and Data Acquisition (SCADA) systems, and similar control systems. Huntsville Center also provides technical expertise of ICS through their additional programs, including the ESS Mandatory Center of Expertise (ESS-MCX), Sustainability and Energy Center of Expertise (CX) for Metering, and the UMCS Mandatory Center of Expertise (UMCS MCX). Additionally, the CS Program is developing the capability to execute RMF requirements for microgrids and medical systems. The CS Program also has the capability to perform studies to assist customers in evaluating if their ICS can undergo and achieve an A&A or if updates are required before applying the RMF requirements.

The CS Project Delivery Team (PDT) is made up of CS Program and project managers, ICS TCX Technical Experts and contracting professionals. Upon initiation of the project, the CS PDT, in coordination with the customer, will develop an acquisition plan and execution schedule for obtaining and maintaining system accreditation.

U.S. Army Corps of Engineers – Engineering and Support Center, Huntsville

P.O. Box 1600, Huntsville, AL 35807 Public Affairs Office 256-895-1694

www.hnc.usace.army.mil

Distribution A - Approved for Public Release - Unlimited Distribution - August 2016

The PDT has various contract vehicles available and will work with various DOD organizations to obtain an ATO and will work with customers to ensure the requirements for maintaining ATOs are understood and can be executed as required. Through up-front coordination and communication with the customer, the CS PDT ensures the customer is aware of all of the requirements for securing their system and what their roles and responsibilities as the end user and system owner will be once an ATO is achieved.

Cybersecurity Systems Scope

After project initiation, the first step will be to validate that the system is compliant with DOD and component specific standards. If the system has been properly maintained and is up to date, the Huntsville Center contractor will be able to start the process requirements for obtaining the ATO. If the system has not been properly maintained and requires updates/upgrades prior to accreditation, the CS PDT, along with the contractor, will work to determine the extent of the updates/upgrades required and provide feedback to the customer to ensure all updates/upgrades are fully documented and understood prior to starting any additional accreditation steps.

As part of the process, the CS PDT will guide the customer in the registration of systems in the required repositories, such as the Army Portfolio Management System (APMS), Ports, Protocols and Services (PPS) List and Enterprise Mission Assurance Support Service (eMASS).

The CS PDT also ensures the contractor fulfills the duties of the contract by providing all required documentation/artifacts, to include, but not limited to, a final hardware/software list, a System Security Plan, Configuration Management Plan, Contingency Plan, Risk Assessment Report, Physical Security Plan, Patch Management Process, a Plan of Actions and Milestones and Continuous Monitoring Plan. The CS PDT will also ensure the appropriate personnel are on site during the independent Security Control Assessor-Validator assessment to assist with answering any questions related to the system. The CS PDT also has the capability to contract out the requirements for executing continuous monitoring after ATO is achieved to ensure ATOs are maintained as required under RMF; or the CS PDT can support the customer in ensuring the continuous monitoring process is understood and executed at the local level.

Why choose Huntsville's Cybersecurity Systems Program? Huntsville Center:

- is home to the ICS Cybersecurity TCX, the ESS-MCX, the Sustainability and Energy CX for Metering, and the UMCS MCX.
- understands the RMF requirement for obtaining and maintaining an ATO.
- provides turnkey solutions that include project management, technical expertise and contract support.
- has a qualified pool of contractors who understand the RMF process and are capable of executing work throughout DOD.
- worked with Fort Hood, Texas, to obtain the only ICS accreditation for a UMCS for the Army. Fort Hood received its ATO under DIACAP in 2015.
- has IAM level II certified cybersecurity specialists in the ICS Cybersecurity TCX to assist with execution of the Risk Management Framework process.

Contract Vehicles

The Cybersecurity PDT supports DOD and other government agencies worldwide by procuring professional services through Blanket Purchase Agreements (BPA) and Indefinite Delivery/Indefinite Quantity (IDIQ) Multiple Award Task Order Contracts (MATOC).