

UNCLASSIFIED



**CLEARED**  
**For Open Publication**

May 30, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

# Continuous Authorization to Operate (cATO) Evaluation Criteria

*DevSecOps Use Case*

29 May 2024

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

UNCLASSIFIED

Contents

Executive Summary ..... 3

Appendix A: DevSecOps Continuous Authorization to Operate: Scope for General Use Cases... 5

Appendix B: DevSecOps Continuous Authorization: Implementation Guidance and Evaluation Criteria ..... 7

Appendix C: DevSecOps cATO Assessment Overview ..... 9

Appendix D: cATO Evaluation Criteria ..... 10

    1.0 Continuous Monitoring ..... 10

    2.0 Active Cyber Defense (ACD) ..... 13

    3.0 Secure Software Supply Chain (SSSC) and DevSecOps ..... 14

        3.1 Authorize the DevSecOps Platform ..... 14

        3.2 Authorize the Process ..... 15

        3.3 Authorize the People ..... 16

Figure 1. Single Authorization Boundary ..... 5

Figure 2. Multiple Authorization Boundaries ..... 6

Figure 3. Software Factory/Production Boundary ..... 6

Figure 4. Assessment Method Overview ..... 7

Figure 5. cATO Memo Competency Assessment Crosswalk..... 9

## **DevSecOps Continuous Authorization to Operate Evaluation Criteria**

### **Executive Summary**

To maintain a competitive advantage, the Department of Defense (DoD) must develop and deploy software with increasing speed and agility, while improving security. Additionally, the DoD must respond quickly to rapidly changing threats through the continuous integration and delivery of capabilities, cybersecurity, resiliency, and survivability. The Department accomplishes this using DevSecOps practices for software development. Software factories (SWF) that use DevSecOps practices can mitigate threats early during software development as well as during operations. To allow software delivery organizations to deploy more secure software faster, the Department will implement a new approach to system authorizations: Continuous Authorization to Operate (cATO).

Continuous Authorization to Operate (cATO) is a modernized authorization process designed to work with software delivery organizations that want to move faster and are willing to adopt the necessary culture change. cATO moves away from solely a document-based, point-in-time technical security assessment approach (though some point-in-time documents are still required), towards focusing on a continuous risk determination and authorization concept by continuously assessing, monitoring, and managing risk. cATO raises the security standard over a traditional Authorization to Operate (ATO) and provides the ability to deploy software more rapidly to the field while improving security. (See Glossary for a more precise definition of cATO.)

A software factory with a cATO is allowed to continuously develop, assess, and deploy software that meets the risk tolerances laid out within a system authorization boundary.

A DevSecOps cATO is based on continual assessment of the processes, the skills of its SWF teams, and the use of a DevSecOps Platform that meets one of the DoD Enterprise DevSecOps Reference Designs, and which implements continuous monitoring, active cyber defense, and the National Institute of Standards and Technology (NIST) secure supply chain guidance.

### **Overview**

This cATO Evaluation Criteria establishes the use cases and guidelines for evaluating a request for continuous authorization for a software factory (for an explanation of a DevSecOps platform and software factory, see [DoD Enterprise DevSecOps Fundamentals](#)).

Additionally, it provides the recommended processes and information required for software factories to generate a cATO package and send to DCIO(CS) for review and approval. Appendix A outlines the two use cases for which requesting a DevSecOps (DSO) cATO is appropriate. Appendix B highlights the baseline guidance and assessment overview as well as the specific information required for the cATO package. Please note that due to evolving requirements, this

**UNCLASSIFIED**

is a living document on the RMF Knowledge Service. Appropriate communities will be notified as updates are made.

**UNCLASSIFIED**

**Appendix A: DevSecOps Continuous Authorization to Operate: Scope for General Use Cases**

Programs or software factories applying for a DSO cATO should already be in one of the following use case categories.

**Use Case 1 (Inside the Software Factory Boundary):** A software factory uses a development, security, and operations (DevSecOps) platform that already has an ATO. Software is developed in that factory and deployed within its production environment (i.e., within its system boundary) as depicted in **Figure 1**. The software factory seeks a cATO that includes its production environment. This is the main use case for a SWF leveraging cATO. *Example: Software developed and put into production using the Platform One (P1) Party Bus. (Note: Information flow includes development, test, and security artifacts).*

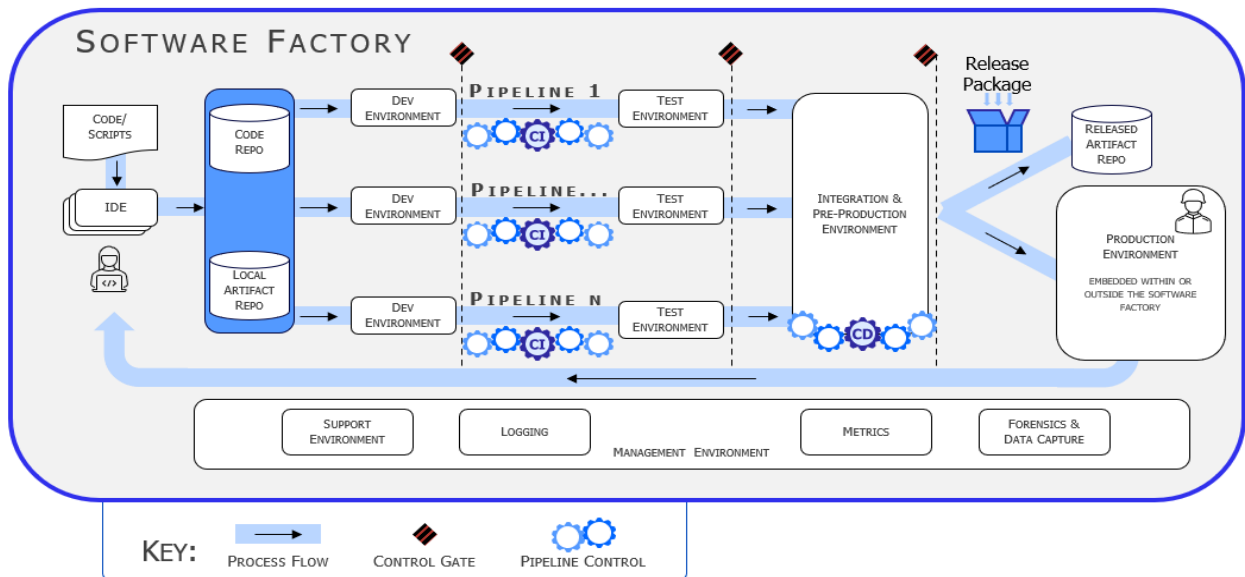


Figure 1. Single Authorization Boundary

**Use Case 2 (Outside the SWF Boundary):** A software factory using a DevSecOps platform that already has an ATO, but the software is deployed into another authorization boundary (e.g., a weapon system) with its own ATO as depicted in **Figure 2**. The software factory seeks a cATO for the factory that allows deployment into the production environment. This involves at least two authorization boundaries and there must be agreements in place to pass software across the boundary and subsequently pass results and feedback back to the software factory. *Example: The Forge Software Factory has an ATO to build software that is then deployed on Navy ships, each of which have their own ATOs.*

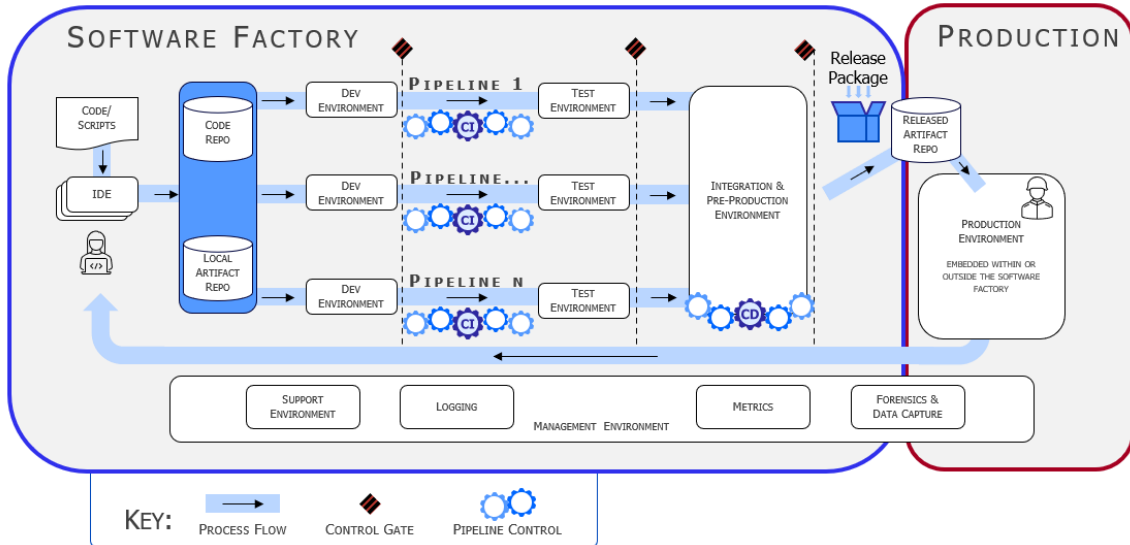


Figure 2. Multiple Authorization Boundaries

An outcome of issuing a cATO for use case 2 is to seamlessly deliver software factory products into the production environment through a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA).

**Figure 3** shows the DevSecOps continuous lifecycle and the delineation between the software factory that is primarily responsible for creating the software product and the associated production environment where the software will execute. (Note: the outer path shows steps in the Risk Management Framework (RMF) process, but this diagram does not directly map these to the lifecycle phases. All the RMF steps must be followed, and the system must be in the **Monitor** phase of RMF, before a system can apply for a cATO.)

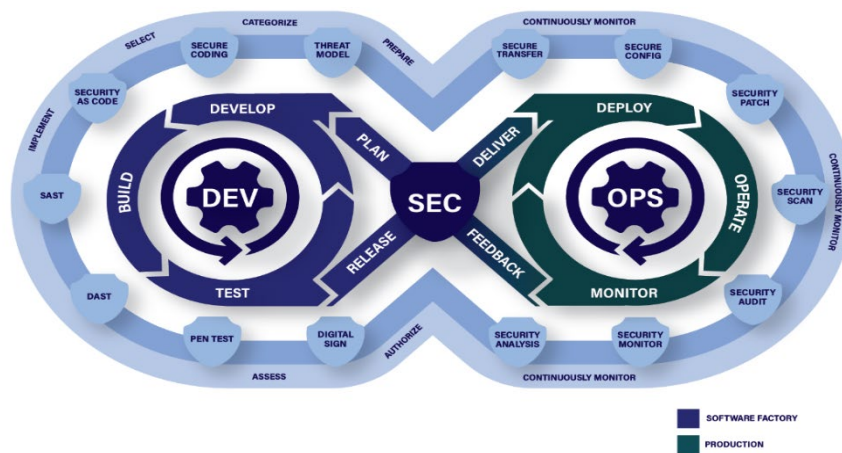


Figure 3. Software Factory/Production Boundary

**Appendix B: DevSecOps Continuous Authorization: Implementation Guidance and Evaluation Criteria**

While the DoD RMF Knowledge Service is the authoritative source for cATO implementation guidance, this appendix provides an overview of how to assess a SWF for cATO along with the requirements to deploy applications outside of the SWF authorization boundary in accordance with [DoD ISCM Strategy](#).

**Figure 4** depicts an overview of the cATO assessment method. The top row shows the related RMF steps: prepare, assess, authorize, and monitor. Other RMF steps (i.e., categorize, select, and implement) take place outside the review process. The next row, with chevrons, indicates the steps taken during the cATO assessment: identify assessors, develop an assessment plan, assess the DevSecOps Platform (DSOP), assess the SWF teams, assess the DSO processes, develop a cATO authorization recommendation, authorize the cATO, and constantly monitor the risk.

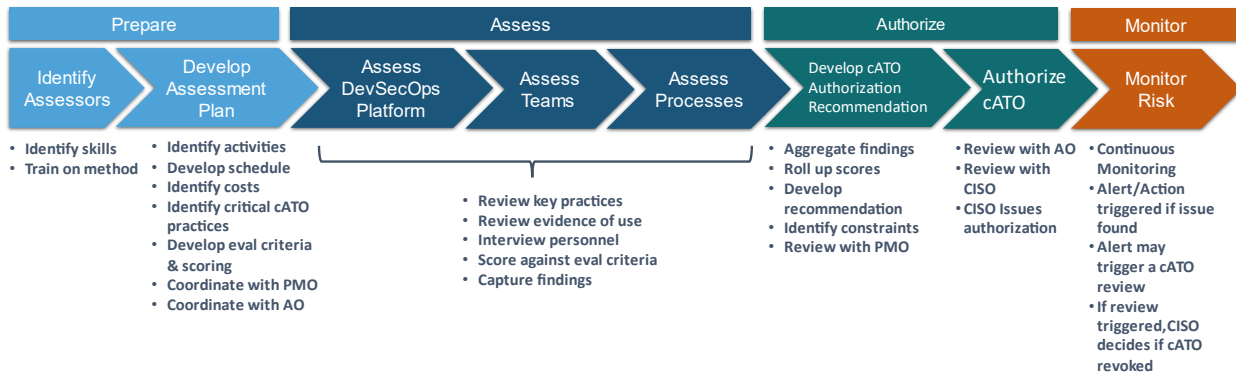


Figure 4. Assessment Method Overview

Software Factory practices required for cATO are informed by the existing RMF authorization to operate assessment and the implementation of continuous monitoring. This assumes that before applying for a cATO, the software factory has already progressed into the monitoring phase of RMF and has a valid ATO. The cATO assessment further evaluates the ‘Prepare’, ‘Assess’, and ‘Authorize’ RMF phases. However, the key to receiving a cATO is having a robust continuous monitoring strategy that includes automated triggers based on approved thresholds within the auditing and incident response plans. The automated triggers and approved thresholds should include both internal and external threats. Additionally, a complete understanding and implementation (or planned implementation) of the shift security left and shield right concept that incorporates vulnerability scanning and compliance checking with detection and response activities to security incidents in real time. This includes tight integration with a Cybersecurity Service Provider (CSSP) and Security Operations Center (SOC) if established. Hosting an environment (development, test, staging, production, etc.) on a cloud requires the deployment of a Cloud Native Application Protection Platform (CNAPP). Once the Chief Information Security

## UNCLASSIFIED

Officer (CISO)<sup>1</sup> grants a cATO, continuous monitoring practices (including the CSSP) monitor the risk. Upon identification of an issue or anomaly, the CSSP, along with the Security Control Assessor (SCA), shall investigate and mitigate as necessary. If the issue or anomaly is outside of agreed upon thresholds, the CSSP or SCA in collaboration with the Authorizing Official (AO) may initiate a review of the cATO. If so, the CISO may decide to revoke the cATO. However, with the approval of the originating Component authorizing official, the system can revert to its original ATO by kicking off a new workflow in the Component's RMF Inventory Tool, if the cATO is revoked.

The approval to implement cATO process within a DevSecOps software factory is granted by following the RMF guidelines identified in CNSSI 1253, NIST SP 800-53 and DoDI 8510.01. In order to receive an approved cATO, the software factory must have a current ATO with no 'High' or 'Very High' unmitigated findings. The cATO analysis will review the existing authorization, further evaluate the continuous monitoring strategy, ensure active cyber defense is implemented properly, assess the DevSecOps and supply chain processes, and validate that they are following cybersecurity supply chain risk management guidance in accordance with [NIST SP 800-161r1](#).

---

<sup>1</sup> Currently, this level of authority is at the DoD-level. Once cATO criteria is standardized for the DevSecOps use case, the DoD CISO will delegate approval authority to the Component CISO or equivalent.






**Appendix C: DevSecOps cATO Assessment Overview**

The three competencies in the memo “Continuous Authorization to Operate (cATO),” February 3, 2022, are (1) Continuous Monitoring (COMMON), (2) Active Cyber Defense (ACD) and (3) Secure Software Supply Chain (SSSC). However, the assessment of this use case is organized into evaluating the DevSecOps Platform, Processes, and People (Teams). This section discusses how to reconcile these two sets of concepts. To be considered for cATO, the environment must ensure:

- 1) The DevSecOps Platform (DSOP) contains essential automation to enable COMMON, ACD, and to support DevSecOps (DSO) tooling for a Secure Software Supply Chain (SSSC).
- 2) Processes are defined for people using, operating, and maintaining the DSOP.
- 3) People are trained on the DSOP and its processes.

The cATO applies to the software factory, which includes the DSOP, and the software produced by the software factory. The processes for using the SWF and DSOP must be clear, and the people must be familiar with all aspects of DevSecOps.

**Figure 5** depicts a high-level crosswalk between these two sets of concepts, showing how they relate. The main columns represent the three competencies, while the rows show the three aspects of the cATO Assessment.

		cATO Memo Competencies		
		COMMON	Active Cyber Defense	SSSC & DevSecOps
cATO Assessment	DSOP 	Generates, analyzes, and displays machine evidence throughout the lifecycle in near real-time	Automation generates evidence and alerts; automatically kills bad containers; CSSP integrated with DSOP team	Automation to secure the supply chain, enforce policy, and enable control gates
	Process 	COMMON process regularly validated and tested	Ongoing active cyber testing, including incident response	DSOP engineering to monitor and improve practices
	People 	Team trained on COMMON automation and DSOP alerts generated by the software factory	Team understands active cyber artifacts and approach to defend; CSSP integrated into team	Cyber dashboard collects relevant information for all DSO stages; all staff trained on DSO process

*Figure 5. cATO Memo Competency Assessment Crosswalk*

## Appendix D: cATO Evaluation Criteria

The following list of activities associated with the Continuous Authorization to Operate (cATO) competencies are what the DoD CISO considers when Component CISOs present systems that are requesting to move into a cATO state.

The presence of these activities will be partly determined through demonstrated use of system-level dashboards, which are a culmination of information received from logging, testing, and the following activities to provide a real-time view of the environment. Components are not limited to the way they conduct the following activities; however, this document offers guidelines to achieving a cATO.

Items in **bold** in this section indicate documents or artifacts that must be delivered as part of the application for cATO package.

### 1.0 Continuous Monitoring

- **cATO Risk Management Strategy**
  - Must include established cATO risk tolerances based on the Components' risk posture guidance
  - Must include process, management, and tracking of insider and external threats
  - IAW DoDI 8510.01
- **System CONMON Strategy**
  - Will be assessed IAW organizational Risk Management Strategy
  - Includes plan to continuously assess and track vulnerabilities on all the system assets within the infrastructure
  - Includes determination of organizationally or software factory-specified metrics (measures) to establish patterns and discern threats such as:
    - Implementation measures to measure execution of security policy
    - Effectiveness/efficiency measures to measure results of security services delivery
    - Impact measures to measure business or mission consequences of security events
  - Includes timelines for continuous monitoring of security controls (automated every hour, minute, second; manual once a year, etc.)
  - Includes tight coupling with auditing and incident response strategies
- **System Authorization Boundary Diagram**
  - Include data flows (including Personal Identifiable Information (PII))
  - Include detailed information for all external connections IAW Appendix E Diagram Requirements of the [DISA Connection Process Guide](#)
- **Business Rules**

- The following are examples of the type of business rules to be established by the system:
  - Closely involve DoDM 8140.03 certified cybersecurity experts throughout the life of the program
  - Define and assign cybersecurity roles and responsibilities
  - Identify and retain Subject Matter Experts (SMEs) to ensure the cybersecurity risk posture of the system is maintained during operations
  - Establish a vulnerability coordination Point of Contact (POC)
  - Align staffing to address detected and identified vulnerabilities
  - AO and designated cybersecurity personnel must have real-time access to the results of testing, scanning, monitoring, and performance metrics at the platform or application level in a mutually agreeable format (i.e., dashboards, alerts, etc.)
  - Identify, assess, prioritize, and share risk information in real time
  - Identify risks in real time and initiate corrective action plans to mitigate them
- **Automated Monitoring Information**
  - Status of dashboarding activities, including a demonstration of the dashboard in operation
  - Must be readily available and as near real time as feasible
  - Includes a dashboard with relevant current information and requirements that helps security personnel perform their tasks
  - Must provide compliance reporting statistics to the Continuous Monitoring & Risk Scoring (CMRS) system of record via automated processes if possible. If not possible, manual reporting is required until automated process is developed.
  - Includes an alerting capability that contacts security personnel when appropriate
  - Demonstrate which security controls are fed into a system-level dashboard view, providing a real time and robust mechanism for AOs to view the environment
  - Helps secure the software supply chain, the software development pipeline and its environment must be monitored as well
- **System Authorization Package Documentation (leveraged from the Component's RMF Inventory Tool)**
  - Security Assessment Plan (SAP)
  - Security Assessment Report (SAR)
  - Risk Assessment Report (RAR)
  - System Security Plan (SSP)
  - ATO memo (Signed)
  - Plan of Action and Milestones (POA&Ms)
  - Update documents in response to CONMON process
    - Security Assessment
      - Ensure it covers the DSOP supporting full lifecycle, including the delivery pipeline and addresses:

UNCLASSIFIED

- Threat modeling and vulnerability analysis
  - Independent verification of assessment plans and evidence
  - Penetration testing
  - Attack surface reviews
  - Manual code reviews
  - Verifying the scope of Testing and Evaluation (T&E)
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - Interactive Application Security Testing (IAST)
- **Continuity of Operations Plan (COOP) / Disaster Recovery Plan (DRP)**
  - **Evidence of COOP/DRP testing**
    - Examples include:
      - Read-throughs, walk-throughs, simulations etc.
      - Backup activities
      - Restoration plan
- **Incident Response Plan**
  - Incident Response Management
    - Evidence of a program in place that includes:
      - Policies
      - Plans
      - Procedures
      - Defined roles
      - Training
      - Proof of communication efforts
    - Examples of evidence include:
      - Read-throughs, walk-throughs, simulations etc.
      - Tabletop exercise
    - Capabilities to detect and respond to attackers
      - Behavior Monitoring evidence
      - Intrusion Detection/Prevention Systems evidence
- **Continuous Vulnerability Management Documentation**
  - Evidence of mitigation
    - Published expectations and timelines for corrective action plans and remediation efforts
    - Published plan to ensure availability of staff and resources
    - Findings tracked using Deficiency Reports and system-level POA&Ms
  - Vulnerability scanning procedures IAW [DoDI 8530.01](#)
  - Leverage process and automation to enable identification of highest priority items and vulnerabilities to remediate (verified through documentation and demonstration)

- Monitor for new threat and vulnerability information IAW DoD and Component level Information Security Continuous Monitoring (ISCM) strategies. Critical and moderate vulnerabilities are documented upon discovery and mitigated within a timeframe acceptable to the AO
- **Audit log analysis**
  - Collect, analyze, alert, review, and retain audit logs IAW NIST SP 800-53 security controls
  - Evaluation of events that could help detect, understand, or recover from an attack, as described in Appendix A of [OMB M-21-31](#)
- **cATO Approval Memo (located on the RMF Knowledge Service (KS))**
  - While cATO approval authority resides with the DoD CISO, this template will be filled out by the cATO Assessment Methodology Working Group and submitted with the Components' cATO package

## 2.0 Active Cyber Defense (ACD)

- **Certified Cybersecurity Service Provider (CSSP)**
  - IAW DoDI 8530.01, Meeting the Evaluator's Scoring Metrics requirements
  - External - CSSP Service Level Agreement (SLA) for both on premises and cloud systems
  - Internal – Documentation of methodology supporting ACD
  - Inherited – Agreements/documentation where integration occurs
  - Outline scope and parameters of CSSP support for on-prem and cloud systems
  - Employ CSSP sensors and tools to detect vulnerabilities
  - **Provide evidence that CSSP received training on DevSecOps principles for the Software Factories that are being monitored**
- **External Assessment Results and Remediation Evidence**
  - A penetration test must be completed on development and operational environments by a qualified third party within 90 days and annually thereafter, with one of the following options, per the AO:
    - Cyber Operations Rapid Assessment (CORA)
    - Red/Blue Team assessment
    - Pen Testing
    - Exception-to-Policy is required for any other type of assessment
  - Some areas of focus include, but are not limited to, the following:
    - Testing the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in the cybersecurity defense posture (people, processes, and technology), and simulating the objectives and actions of an attacker.
    - Testing the authorization boundary IAW [DoDI 8531.01](#), in search of weaknesses that would allow unauthorized access.

- Provide a Vulnerability and Penetration Assessment
- AO provided results with findings and planned mitigations.
- Updated document POA&Ms where appropriate
- Lessons Learned tracking
- **Security Testing and Documentation**
  - Security testing should be conducted on an ongoing basis and test against adversary tactics and techniques based on real-world observations
  - Strategy and budget for automated cybersecurity testing resources
  - Documentation of the ongoing iterations of cybersecurity analysis and penetration testing
  - Documentation and evaluation of the impact of system or environment changes to the cybersecurity defense posture

### **3.0 Secure Software Supply Chain (SSSC) and DevSecOps**

#### **3.1 Authorize the DevSecOps Platform**

- **Use of a DevSecOps Platform (DSOP) that implements an approved DevSecOps Reference Design, or implementation of an approved DevSecOps Reference Design**
  - Identify the DevSecOps Reference Design to which the DSOP adheres
  - Approved DoD Enterprise DevSecOps Reference Designs are posted to the [DoD CIO public library](#)
- **Software Bill of Materials (SBOM)**
  - Provide a SBOM for the DSOP with a statement of how it was developed
  - Provide an automated export of the SBOM for applications/products passing through the DSOP
  - Specify the SBOM format and how often it is generated
    - SBOM should be in one of the common formats:
      - Software Package Data Exchange (SPDX)
      - Software Identification Tags (SWID)
      - CycloneDX
      - However, the format has not yet been mandated. SBOM is currently undergoing regulatory action, Defense Information Systems Agency (DISA) Federal Acquisition Regulation (FAR) is the lead
  - Maintain an archive of SBOMs for products passing through pipelines. This can be kept in the same area as the assessment evidence (e.g., results of security tests) for the products
  - Explain how the SBOMs are analyzed. If a new cybersecurity vulnerability appears in the Common Vulnerabilities and Exposures ([CVE®](#)) system, explain how the organization applies it to the SBOMs
- **Activities and Tools Mapping**

- Based on the [DevSecOps Activities and Tools Guidebook](#), provide the mapping of the required and preferred DevSecOps activities to the system's implementation.
- Include any additional documentation listed with the mapped activities in the Activities and Tools Guidebook
- Provide Activities and Tools Mapping POA&Ms/Roadmap to show continuous improvement
- Provide demonstration of various activities listed within the Activities and Tools Guidebook (selected activities determined during the cATO evaluation)
- **Cloud Native Application Protection Platform** - Employ an integrated set of security and compliance capabilities to secure and protect cloud-native applications across development and production to include:
  - Artifact Scanning:
    - Software Composition Analysis to review artifacts to find open-source libraries included. This should be addressed in the creation of the SBOMs.
    - Application Security Testing such as SAST, DAST, and IAST
  - Cloud Configuration:
    - Cloud Security Posture Management (CSPM) for continuous monitoring, detection, and remediation of cloud security misconfigurations.
    - Cloud Infrastructure Entitlement Management (CIEM) for management of access rights, permissions, or privileges for the identities of a single or multi-cloud environment.
    - Infrastructure as Code (IaC) Scanning to find security flaws before pushing to production.
  - Runtime Protection:
    - Cloud Workload Protection (CWPP) to provide runtime enforcement
    - Cloud Detection and Response (CDR) to provide advanced threat detection, incident response, and continuous monitoring capabilities specifically designed for cloud environments.

### **3.2 Authorize the Process**

- Reliance on Infrastructure as Code (IaC) and Configuration as Code (CaC) to avoid environment drift
- **Control Gate and Guardrail Analysis**
  - These processes should be described in the Incident Response Management section above
  - Provide a description of each control gate and what triggers cause the gate to close and open. This should include what triggers an alert and how to respond to that alert
  - Demonstrate each control gate in action (this may be in a non-production environment) or provide screen shots of control gate output as displayed in a dashboard

- Provide a description of each guardrail and the process that occurs when something is out of the risk tolerance for each guardrail

### **3.3 Authorize the People**

- **Verification of appropriate training for each member of the team(s), based on their role(s)**
  - Provide an organization chart showing the roles within the DSO Team
  - Demonstrate appropriate separation of duties and least privilege are applied to all personnel
  - Periodically conduct Tabletop Exercises with the whole team and produce **After Action Reports**
    - Exercises should include:
      - Security incident response procedures
      - Standard procedures for the DSOP, including how to respond when a control gate triggers
      - How to respond to a security alert
      - Requests for elevated privileges
- **The organizational DevSecOps education, certification, and training process is documented.** Documentation need not be text documents but may be in online learning management tools that assessors can view. Possible areas of training include Agile, DevSecOps, secure coding, security automation tools, interpreting vulnerability scanning reports, cATO method, etc.
  - The team members are trained in the cATO method:
    - Trained on the appropriate version of the DoD Enterprise DevSecOps Reference Design.
    - Trained on the security automation tools and how they are used.
    - Trained on the Continuous Integration/Continuous Delivery (CI/CD) control gates, promotion rules, and the established risk tolerances.
    - Trained on the resolution / adjudication of security findings that result in exceeding the risk tolerances.
    - Ability to perform root cause analysis of “critical” and “substantive” security findings.
    - Trained in continuous monitoring feedback loops for ensuing continuous risk monitoring against tolerances.
    - Trained in the establishment of POA&M and security dashboard monitoring in a DevSecOps environment.
  - Verification of appropriate training for each member based on their role on the Product/Application Team, DSOP Team, or Security Team
  - Verification of cybersecurity team member qualifications in accordance with DoD DoDM 8140.03



UNCLASSIFIED

- Document cross-functional team training and shadowing
- **Insider Threat Monitoring**
  - Validate an insider threat working group is established, active, and chaired by senior leadership
    - Validate insider threat working group identifies critical areas for review along with thresholds for analysis
  - The below concepts can be used to protect against insider threats:
    - Separation of duties
    - Paired programming
    - Least privilege management with respect to containers/cloud environments
- **Onboarding/Offboarding**
  - **An onboarding/offboarding process is defined** for new team members based on their role.
  - **Show evidence that all personnel have gone through the onboarding/offboarding process**, without regard to their rank or position.

## Glossary

**Authorization boundary** “All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.” NIST 800-37r2.

**Authorizing Official (AO)** is “a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.” NIST 800-37r2.

**Authorization to Operate (ATO)** is “the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.” NIST 800-37r2.

**Continuous Authorization to Operate (cATO)** is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system’s cyber posture.

**Continuous Integration/Continuous Delivery (CI/CD) Pipeline** is the process workflows and associated tools to achieve the continuous integration and continuous delivery of software with maximum use of automation.

**Control gate** is a defined point in the project lifecycle when specific requirements, called **exit criteria**, must be met to move to the next phase in the lifecycle. Exit criteria include functional, security, and non-functional criteria.

**DevSecOps** is a software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development: plan, develop, build, test, release, deliver, deploy, operate, and monitor.

**DevSecOps Platform (DSOP)** is the set of tools and automation that enables a software factory. It includes the ability to create DevSecOps pipelines with control gates, and to deploy software into development and test environments. It may also deploy into production, depending on the production environment. Use of a DevSecOps platform is encouraged to accelerate development, delivery, and authorization. DoD Enterprise DevSecOps Reference Designs for a DSOP may be found [here](#).

**ISCM** is defined as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.” NIST SP 800-137.

**UNCLASSIFIED**

**Software Factory** is a software assembly plant that contains multiple pipelines, which are equipped with a set of tools, process workflows, scripts, and environments, to produce a set of software deployable artifacts with minimal human intervention. It automates the activities in the develop, build, test, release, and deliver phases. The software factory supports multi-tenancy.

**System** is any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. NIST 800-37r2.