IT Security Procedural Guide: OCISO DevSecOps Program CIO-IT Security-19-102

Initial Release

September 26, 2019

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Release – September 26, 2019				
N/A	ISE	New guide created to integrate security into DevOps teams.		

Approval

IT Security Procedural Guide: OCISO DevSecOps Program, CIO-IT Security-19-102, Initial Release is hereby approved for distribution.

X e-Signed by Bo Berlas
on 2019-09-27

Bo Berlas
GSA Chief Information Security Officer

For questions concerning the DevSecOps Program contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE), at ociso-devsecops@gsa.gov

For questions concerning GSA Policy and Compliance contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP), at ispcompliance@gsa.gov.

Table of Contents

1 Introduction 1
2 Purpose 1
2.1 Improve Security and Quality 1
2.2 Facilitate a cultural shift 1
2.3 Reduce silos and communication barriers 1
2.4 Provide security services through an integrated engineer 1
3 Scope 2
4 Defining DevSecOps 2
4.1 What DevSecOps Is Not 3
4.2 What DevSecOps Is 3
5 ODP Governance Model 3
5.1 Roles and Responsibilities 3
5.1.1 ODP Security/DevSecOps Engineer 4
5.1.2 DevSecOps Application Team 5
5.1.3 System Owner 5
5.1.4 ODP Team 6
5.1.5 Chief Information Security Officer 6
5.2 Overview of Processes and Procedures 7
5.3 Communication, Report, and Organizational structure 7
5.4 IT Security Metrics 9
6 Operational Model 11
6.1 People 12
6.2 Processes 12
6.3 Technology 13
7 Prerequisites for Initial Integrations 13
7.1 Uses a Platform 13
7.2 Uses a Continuous Integration and Continuous Deployment (CI/CD) Pipeline 14
7.3 Uses Automation 14
7.4 Leverages a Robust API 14
7.5 Commitment to Abide by the Operational Model 14
8 How to Initiate an ODP DevSecOps Integration 14
9 Rules of ODP DevSecOps Engagement 14
10 ODP Resources / Links 15

Figure 5-1. OCISO DevSecOps Governance Model 3
Figure 5-2. Security Engineer Communication and Reporting 8
Table 5-1 - Key Security Control/Capability Gaps 9

1 Introduction

With more teams at the General Services Administration (GSA) leveraging Development and Operations (DevOps) practices, ensuring effective security practices has become paramount. The Office of the Chief Information Security Officer's (OCISO) DevSecOps Program (ODP) aims to ensure that GSA teams who practice DevOps adopt security forward thinking. The program facilitates the creation and operation of DevSecOps teams in GSA.

2 Purpose

This guide serves to establish the ODP throughout GSA's development, operations, and security organizations. The program establishes security as the third component into the DevOps teams, effectively creating DevSecOps teams in GSA. The ODP will be managed and run by OCISO Security Engineering (ISE) division. This procedural guide will establish a process and operating principles for ODP. The following subsections define program goals.

2.1 Improve Security and Quality

The ODP aims to ensure security is considered and implemented in all design and operational phases. The ODP aims to provide full security support in areas including Incidence Response, Security Automation, and Compliance.

2.2 Facilitate a cultural shift

Security is often associated with compliance at GSA. While an important part of the system life cycle, security is not just compliance. The ODP aims to shift the agencies thinking of just Authorization to Operate (ATO)'s and Compliance to everyday considerations and operations. The ODP is intended to have everyone adopt a "How can we do this securely?" mindset. Furthermore, we aim to shift the thinking of "security as engineers over there" to they are part of our team.

2.3 Reduce silos and communication barriers

Too often, the OCISO DevSecOps programs only engagement with system teams occurs when there is an incident or when there is an assessment. The lack of sharing information and code leads to "rebuilding the wheel" development cycles. The ODP aims to provide a simple and consistent communication channel where solutions, code, and more can be shared amongst teams to make development cycles efficient and secure.

2.4 Provide security services through an integrated engineer

Most often OCISO security services are only available during Assessment & Authorization (A&A), Incident Response and in support of limited ISSO functions. Security services are provided through different divisions and teams. By placing an integrated security engineer in the DevSecOps team, the OCISO DevSecOps program can deliver all security services through the integrated engineer. The integrated engineer could be your ISSO and can provide services for ODP security-related functions.

In addition to the program goals, this document will define the following areas:

- Defining DevSecOps
  - What does DevSecOps mean and how does the ODP define it?
- Prerequisites
  - What are the requirements for your team to successfully integrate with the ODP
- Governance
  - What are the governing principles of the ODP?
  - Items such as:
    - Roles and Responsibilities
    - Policy and Procedure
    - Communication, Report, and Organizational structure
    - Metrics
- Operational model
  - What are the guidelines and guardrails of the program?

3 Scope

The OCISO DevSecOps Program is available to all GSA cloud-based information systems. The ODP resources and services may consist of security guidance, providing DevSecOps code/documentation/reference architecture, and/or integrating a security engineer into your team.

4 Defining DevSecOps

DevSecOps is an iteration of the term DevOps. DevOps originates from the idea of combining two previously siloed groups, Development and Operations. Then by using practices, tools, and a new cultural approach, teams can build and deliver applications and/or services at greatly increased speed and at scale. DevSecOps makes security an equal partner in the workflow.

As with DevOps, DevSecOps can have different definitions depending on the industry or system owner. It can range from “simple cross-functional collaborative team including IT security personnel” to “Self-sustained, highly agile, self-managed team driving cultural shift”. While this document will not establish a universal definition of DevSecOps, it will define how the ODP defines it.

At a high level, the ODP defines DevSecOps as “Integrating security into all the workflows and practices of DevOps.” Or as DevSecOps.org’s statement reads “everyone is responsible for security” Due to the complexity and nuance of DevSecOps, the following sections expand on defining what it is and what it is not.

4.1 What DevSecOps Is Not

- A set of security tools
- Solely automating a security function
- Solely security compliance

4.2 What DevSecOps Is

- Embracing a culture where everyone is responsible for the security
- Considering security in all aspects of the system life cycle. From the first system kickoff to the final decommissioning.
- Using the already existing DevOps practices and methodologies to implement, enforce, and monitor security.
- Implementing paved roads. Paved Roads include items such as pre-approved architectures, processes, capabilities, solutions, etc. that wouldn't need additional review or approvals.

5 ODP Governance Model

The ODP governance model consists of four major areas. Each area sets foundational principles to be followed by each stakeholder. To adopt an agile culture of DevSecOps, these foundational governing principals and their details can be revisited for each engagement and will be finalized as a mutually agreed set of principles/ROE between OCISO and integrated teams.

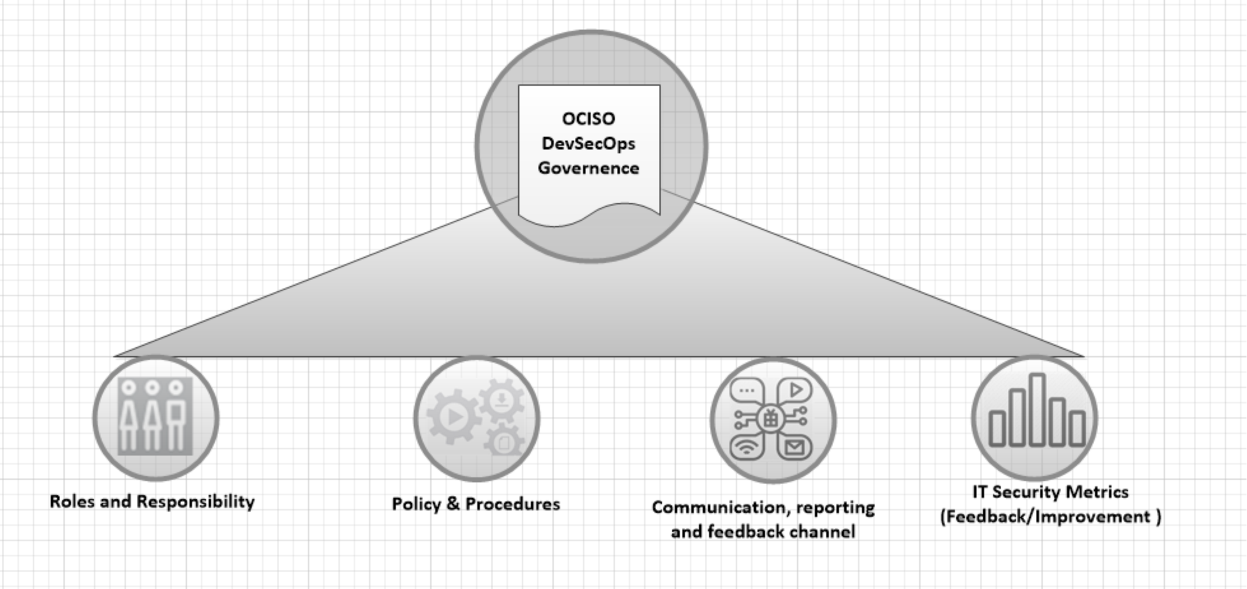
OCISO
DevSecOps
Governence
Roles and Responsibility
Policy & Procedures
Communication, reporting and feedback channel
IT Security Metrics (Feedback/Improvement)

Figure 5-1. OCISO DevSecOps Governance Model

5.1 Roles and Responsibilities

Well defined roles and responsibilities are imperative for cross-functional DevSecOps teams. Teams desiring integration with the OCISO DevSecOps program shall adhere by these high-level roles and responsibilities. However, to support agility and based on the maturity of the team, these roles and responsibilities will be reviewed prior to each engagement. Mutually agreed upon roles and responsibilities will be finalized between the ODP program and the integrated DevSecOps teams.

The ODP integrated engineer's priority is security focused on technical design and implementations. The ODP program is designed to provide an integrated working model in a collaborative way with GSA DevOps teams. The ODP program will NOT change any compliance or ATO related to existing security policy and procedural guidelines/practices. However, ODP will encourage and adhere to any changes in the future.

The ODP program intends to keep compliance and operational security domains separate to create a more collaborative working environment between the integrated engineer and DevSecOps teams. It is the system owner's responsibility to maintain a level of separation between security design, engineering, operations, and compliance related activities. The ODP program establishes a collaborative working environment by integrating SecDevOps security engineers into the development teams ensuring security becomes a part of DevOps practices.

5.1.1 ODP Security/DevSecOps Engineer

The ODP Security/DevSecOps Engineer serves as the overall Security SME/Champion for the assigned system. (The engineer assigned to this role could also be designated as the traditional ISSO, upon agreement between ODP and integrated team.)

Responsibilities:

- Works with the system team on all aspects of system security in collaboration with the DevSecOps team which includes security designs, security architecture, implementation, operations, and compliance.
- Engages directly with integrated DevSecOps team in solution design, sprint planning, story creation, defining acceptance criteria, and to ensure security requirements are properly addressed in early phases.
- Interprets security requirements, policy, standards, control statements and its applicability for DevSecOps team and/or system implementation.
- Acts as liaison between the security organization and divisions as needed.
- Engages directly with ODP for security-related questions, clarification, decision points, reviews, etc., as needed.
- Establishes a process to identify which changes need security review and approvals.
- Integrates into change management process as security reviewer.
- Collaborates with system team for security code review, compliance impact analysis, liaison with OCISO for security approvals.
- Establishes and maintains a security-related operating procedure for DevSecOps teams such as rapid risk assessment procedure, a procedure for engaging GSA IR team, etc.
- Provides support, code and consulting for integration with security tools and services.

- Actively engages in operational security by solution, coding and/or code review, initial investigation on alerts and incidents, vulnerability identification and mitigation as needed in collaboration with DevSecOps team.
- Collaborates with the System Owner for developing and maintaining the System Security Plan (SSP) and Plan of Action & Milestones (POA&M).
- Collaborates with other DevSecOps teams and security champions to build reusable security code components, collaboration to build code library, security automation, security checklist, do's/don'ts, security wiki, etc.

5.1.2 DevSecOps Application Team

The DevSecOps Application Team (team includes integrated security engineer) provides the day to day operations of all the aspects of the system and/or application. It includes development, security, and operations. The DevSecOps Application Team could have different SME within the team, but overall the team always owns all aspects of the system and/or application including security and compliance.

Responsibilities:

- Everything for their system/application. That is designing, development, coding, operation, security, compliance, documentation, etc. based on business objectives and mission.
- Security design, implementation, alerts and incident monitoring, security documentation and compliance.
- Adopting an operational model, which supports continuous releases, upgrade and changes while fully maintaining security posture, principle, and compliances of the application/system.
- Develops standard operation procedure for security monitoring, investigating alerts take corrective action and/or engage incident response team as needed.

5.1.3 System Owner

The system owner provides overall ownership of a system/product/application including security and compliance.

Responsibilities:

- Provides clear product vision and roadmaps.
- Provides high level product requirements, design/architecture consideration, and design/operational decisions.
- Sets priorities, manages DevSecOps team, time, and resources.
- Manages task and priorities of security engineer for allocated time on each sprint cycle.
- Manages the onboarding, integration, and establishment of a working model for effective collaboration between security engineer and existing DevOps team.
- Ensures ODP integrated engineer's priority is security focused design, engineering, operation, and implementation.
- Resolves priority conflict between security/compliance requirements and application release/development priorities.

- Measures and monitor program success against established/agreed metrics continuously.
- Develops a plan and executed security requirements, checklist, guardrails, policy, and procedure agreed as part of this integration.
- Collaborates with OCISO leadership (e.g., CISO, OCISO Directors, ISSM), along with integrated security engineer for high-level decision making, review, and approvals as needed. (Especially when such decisions are outside of established standards).

5.1.4 ODP Team

The ODP Team provides authoritative decisions to DevSecOps teams on questions, guidelines, and reviews. The ODP Team acts as a security advisor, provides day to day support and a collaborative platform for all security engineers, DevSecOps engineers, and security champions.

Responsibilities:

- Runs collaborative platform, scrum, Trello, question/clarification rosters to support integrated team, security engineer and security champions.
- Develops and maintains DevSecOps security checklists, wiki, implementation guides, and processes and procedures.
- Provides authoritative guides, decisions, and approvals for questions and requests, received by security engineer, security champions and/or integrated DevSecOps teams.
- Build repetitive decision-making processes and guidelines to empower security engineer and security champions.
- Works closely with CISO and/or CISO designee for authoritative decision making, when the team needs additional guidance.
- Works closely with CISO and/or CISO designee for A&A related assessment and final sign-off.
- Works with other OCISO divisions as needed.

5.1.5 Chief Information Security Officer

The Chief Information Security Officer provides implementation and maintenance of the IT security program, including the ODP. The Chief Information Security Officer also provides a final authoritative decision on all questions, concerns, and guidelines requested by the ODP.

Responsibilities:

- Designates role or personnel to provide authoritative decisions, approvals, and guidelines for questions, concerns, approvals, and reviews requested by security engineer, security champions and integrated DevSecOps teams.
- Provides final authoritative decision on all questions, concerns, and guidelines requested by the ODP team, security engineers, and security champions.
- Provides risk-based decisions and ATO sign-off for integrated DevSecOps team systems/applications, as per existing policy and procedural guidelines.

5.2 Overview of Processes and Procedures

The ODP will identify the processes, procedures, and technical guidelines that stakeholders shall adhere to. Initially, the ODP will propose core processes and procedures. As the team integrates and matures, the core processes and procedures will be refined and enhanced to provide improved support to the teams.

Processes, procedures, and technical guidelines that will be developed include:

- Standard security architecture and implementation guides for different platforms available for GSA teams.
- Pre-approved standard architecture and processes (paved road vs slow road).
- Checklists for security guard rails.
- Checklists for security implementation through a CI/CD pipeline.
- Processes for rapid threat/risk assessment.
- Security review processes for change management/production release.
- Processes for monitoring security events and engaging the IS incident response team.
- Process for incident response playbook testing and live fire exercises.
- Process for reviewing documentation, reviewing, and publishing security code components (for facilitating code sharing between teams).
- Process for documenting security engineering decisions and precedence.
- DevSecOps change management and review process.

Listed below are current lists of ODP approved processes, procedures and/or checklists for integrated DevSecOps teams:

ODP Security Checklist For AWS V1 :

- Basic security checklist for ODP integrated teams using an Amazon Cloud Environment.

5.3 Communication, Report, and Organizational structure

The ODP is a cross-functional program, which demands cross-team collaboration, communication, and organizational structure. Integrated ODP Security/DevSecOps Engineer or security champions will play a cross-functional role as outlined below.

Shall report/communicate to product/system owner for:

- Day to day tasks tracked in Trello, sprint-based goals/progress, and project backlog grooming status.
- Tasks that shall be allocated based on agreed rules of engagement and percentage of work hours assigned for the engagement.
- Results from Internal security review, change/code review, security design review, vulnerability findings, remediation, etc.
- Status of security-related questions, feedback, reviews which needs support from other OCISO resources and divisions.

- Items blocked or on hold.

Shall report/communicate to the ODP for:

- Security-related initiatives, implementation status of security checklist, guardrails, compliance, vulnerability, etc.
- Integration of security tools and processes.
- Any incident and related investigations.
- Any sprint blocker that is directly related to pending action on any OCISO division.
- Results of agreed security metrics.
- Compliance status, issues, findings, and POA&M.
- Questions or clarifications related to security engineering, design, and compliance.

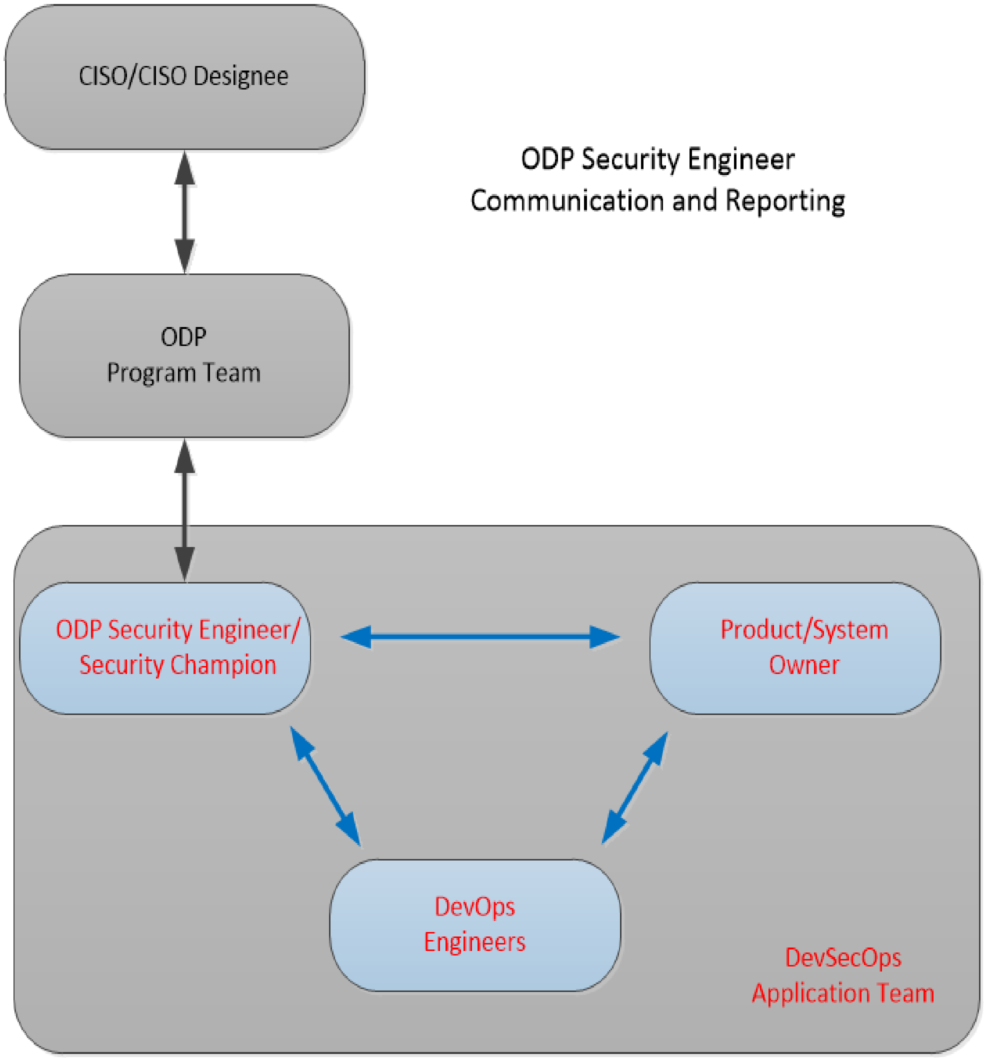
CISO/CISO Designee
ODP Security Engineer Communication and Reporting
ODP Program Team
ODP Security Engineer/ Security Champion
Product/System Owner
DevOps Engineers
DevSecOps Application Team

Figure 5-1. Security Engineer Communication and Reporting

5.4 IT Security Metrics

The ODP will work with the teams to identify and track a set of metrics to measure program success. This allows the teams to report to leadership (both from the application team and from OCISO) with data and artifacts as evidence of the overall success of the integration. Furthermore, these metrics will be used by the ODP internally to measure effectiveness and areas for program improvement. Metrics might vary for different integrations based on the project, application, and other factors.

The final set of selected metrics for each integration should be clearly understandable and measurable in quantitative values or in checklist format (yes/no), and agreed to by ODP and application team management. See below for a list of examples to prompt discussions for establishing metrics.

Table 5-1 - Key Security Control/Capability Gaps

Key Security Control/Capability Gaps		
Metric	**Description**	**How to measure?**
Multi-Factor Authentication (MFA)	All authentication points use MFA for authentication as per NIST 800-63-B.	Checklist (Yes/No/NA)
Data encryption	All sensitive data (PII, PCI, authenticator or classified as sensitive by business) is encrypted with FIPS approved cipher. It includes data stored in databases (table, field, or column), flat files, pdf, images, backups, logs anything that could have sensitive data.	Checklist (Yes/No/NA) / Percentage of database meeting requirement.
Uses of outdated and/or unsupported software exist	Unsupported (both COTS and open source) software or tools are not in use	Checklist (Yes/No/NA) / Count of outdated and/or unsupported software
Residual OIG/Financial Audit Findings (if any)	Pending findings from last OIG/Financial Audit	Count of pending findings from the last audit that has not been remediated, must be included in the systems POA&M

Key Security Control/Capability Gaps		
A&A Status	Current ATO status	Full ATO or LATO/ Remaining months to expire
Cyber Hygiene		
Operating System Hardening	The adoption and implementation of the GSA hardening guides or CIS guides if no GSA guide is in place.	FISMA metrics for compliance reporting of hardening scans. (Percentage)
Average patching Cycle	The timeframe for how often and regularly applications and operating systems are applying patches.	The average number of days between the application of security patches. (Number Count)
GSA recommended Security agent in use.	The full adoption of the security stack.	Checklist (Yes/No/NA)
Pentest and Bug Bounty	Submit the system regularly tested for attack vectors, exploits, vulnerabilities, etc.	Number of Pen Tests per year/ Existence of established bug bounty program (Yes/No/NA)
Integration into a Continuous Monitoring Program. * *When CDM Phase#3 program is officially launched.	Having the system integrated into a continuous monitoring program where items on this list are measured in real time.	Checklist (Yes/No/NA)

Key Security Control/Capability Gaps		
Count of high and critical vulnerability open for more than 30 days.	Provides picture of system environment from a vulnerability management perspective	The number count of high and critical vulnerability open for more than 30 days based on scanning report. **Note:** These vulnerabilities need to be included in the systems POA&M.
DevSecOps Maturity		
Patching methodology	Patching is performed by replacing OS image	Checklist (Yes/No/NA)
Uses of security unit/integration tests	Are security unit/integration tests written in code and tested as part of the pipeline?	Checklist (Yes/No/NA)
Number of security unit/integration tests for NIST Controls	Number of security unit/integration tests written in code for NIST Control validation	Count of security unit/integration tests. For counting purposes, each sub-section of NIST control language is one count.
SAST (static analysis security testing) is integrated into CI/CD pipeline	Static code analysis in the pipeline	Checklist (Yes/No/NA)

6 Operational Model

GSA teams integrated with ODP shall adopt a general DevSecOps operating principle and methodology outlined in three broad categories of people, process and technology.

6.1 People

- Team structure should support DevSecOps working model, which is a self- sustained, self-managed, integrated team with full responsibility for the development, security, and operation.
- Formation of DevSecOps team by integration with ODP. ODP program integrates security engineer with application team for building GSA DevSecOps teams.
- No contractual or other limitations which force breaking down of development, operation and security ownership into multiple teams working in silos.
- Clear role and ownership for system owner on day to day decision making, prioritizing, technology choices, setting long term and short-term product vision, conflict/priority management.

6.2 Processes

- ODP mandates the adoption of mandatory OCISO DevSecOps security checklist for ODP integrated teams. Listed below is the mandatory ODP process and/or security checklist as of now.
    - **ODP Security Checklist AWS V1: Basic mandatory security checklist for ODP integrated team using Amazon Web Services**

- ODP will build DevSecOps specific process and procedures in collaboration with integrated teams. Upon approval by GSA OCISO CISO, ODP integrated teams shall adopt and implement the ODP process and procedural guides. Advisory process and guides are not mandatory but are highly recommended by ODP. Examples of the process to be developed as ODP matures may include:
    - The change management process for DevSecOps team.
    - Continuous security review, response and release process for DevSecOps teams.
    - Process for reporting security metrics.
    - Process for code sharing and collaboration with other DevSecOps teams.
    - Process for updating, submitting contents on ODP security Wiki, readme pages by integrated teams.
    - The rapid risk assessment process.
    - A standard architecture for specific platforms.
    - OCISO Security Checklists.

Note: *This process, procedure and security checklist does not replace an ATO requirement. These are supplementary specific to the DevSecOps program. The ODP program is designed to be agile and flexible to create a more collaborative working model. The ODP team will work with integrated teams to develop these processes that work for existing and new teams. There could be different processes for different teams based on their product, scale, and maturity.*

6.3 Technology

ODP does not mandate the use of any specific tools or technology. However, ODP highly recommends the use of tools and technology that is already in use at GSA, have existing approvals and are market leaders, for obvious reasons such as skill transferability, widely available content, quick adoption, and support. A list of GSA approved tools and technology is available in GSA EA Analytics & Reporting (GEAR) IT Standards List webpage. A list of FedRamp approved SaaS offerings is available at the FedRamp website.

- Adopt cloud first principle. Use public cloud offering such as AWS for your systems build. Use native cloud services as much as possible.
- Adopt approved, standard architecture when available.
- Adopt Infrastructure as Code principle. Uses of tools such as terraform, packer and CloudFormation for provision of infrastructure.
- Adopt configuration management automation. Uses of tools such as Ansible, Chef, puppet for configuration management.
- Version Control and centralized code repository. Uses of github for version control and centralize code repository.
- Adopt uses of CI/CD pipeline, for continuous integration and delivery. Uses of tools such as Jenkins or CircleCi for CI/CD pipeline.
- Adopt project management tools such as Trello, Jira, Slack, GitHub issues, etc. for project management, communication, and collaboration.
- Adopt Security as Code principle. Uses of above listed and/or additional tools for security infrastructure test and security unit test in an application.
- Uses of CI/CD pipeline for security check and testing such as static analysis security testing (SAST) and static and dynamic analysis security testing (DAST), anti-pattern check, security unit test, etc. These implementations can mature over time.
- Uses of existing, enterprise security tools and offering from OCISO. Examples include offering such as Nessus vulnerability scanner, Cylance AV, FireEye, etc.

7 Prerequisites for Initial Integrations

Before a team can request an ODP engineer to integrate with them, they must meet the following prerequisites. These can already be established or the team must be willing to commit and put them in place.

7.1 Uses a Platform

The ODP defines a platform as any plane of infrastructure where code and an Application Programming Interface (API) can be leveraged. This could be any public cloud service, such as Amazon Web Services, Microsoft Azure, or Google Cloud Compute (GCP).

7.2 Uses a Continuous Integration and Continuous Deployment (CI/CD) Pipeline

To effectively practice DevSecOps, the team needs to have or plan on using a CI/CD pipeline. The ODP will champion using infrastructure and security as code as much as possible to make code authoritative.

7.3 Uses Automation

The team must have the use of automation and security automation as a priority in its development process. To effectively practice DevSecOps, the team must already embrace a "How can we automate this?" mentality.

7.4 Leverages a Robust API

The team's application stack must have a robust and mature API. Having a robust API allows the team to extract critical data, facilitating programs such as Continuous Monitoring.

7.5 Commitment to Abide by the Operational Model

Your team must have a commitment to follow the Operational Model detailed in this document.

Note: *Even if prerequisites are met, the ODP will review the compatibility of the team with our goals and resources and make a final determination of team integration.*

8 How to Initiate an ODP DevSecOps Integration

- Send an email to OCISO DevSecOps Program Team (ociso-devsecops@gsa.gov).
- The ODP will review the request and schedule a call for further discussion, with a turnaround of 3-5 business days.
- If a team meets our basic prerequisites, the ODP will schedule a kickoff meeting to discuss the particulars of integrating with your team.
- OCISO DevSecOps program is designed to fit the agile working model and fluid requirements. ODP is flexible for any discussion within constraints of core security requirement and resource availability.

9 Rules of ODP DevSecOps Engagement

- Commitment to the Governance Model.
- Commitment to identify and use security metrics.
- Provide reports on metrics.
- Commitment to abide by ODP mandatory processes where applicable.
- Commitment and bias priority towards Infrastructure as Code and Security as Code.
- Commitment to share code, process, technology, and know-how with other GSA teams.

- Identify the level of effort needed from integrated security engineer in terms of percentage of the work week.
- Notice of agreed upon weeks from either side to end engagement.
- Agreement between the principles.

10 ODP Resources / Links

Mandatory security checklist for ODP integrated team using Amazon Web Services (**ODP Security Checklist AWS V1**)