NIST National Cybersecurity Center of Excellence

Secure Software Development, Security, and Operations (DevSecOps) Practices

August 27, 2025

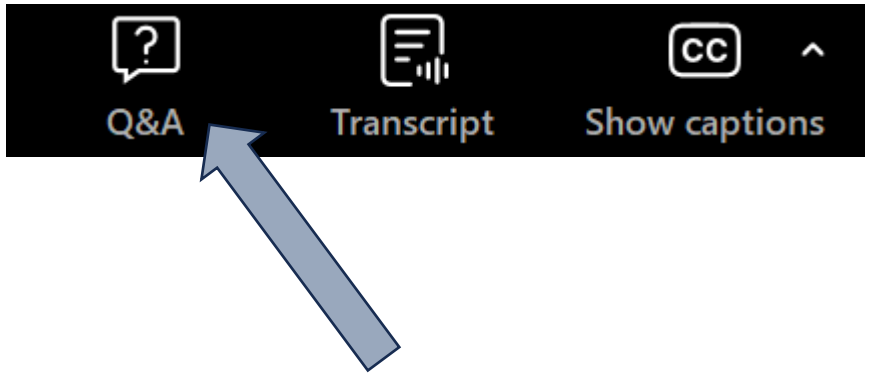
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

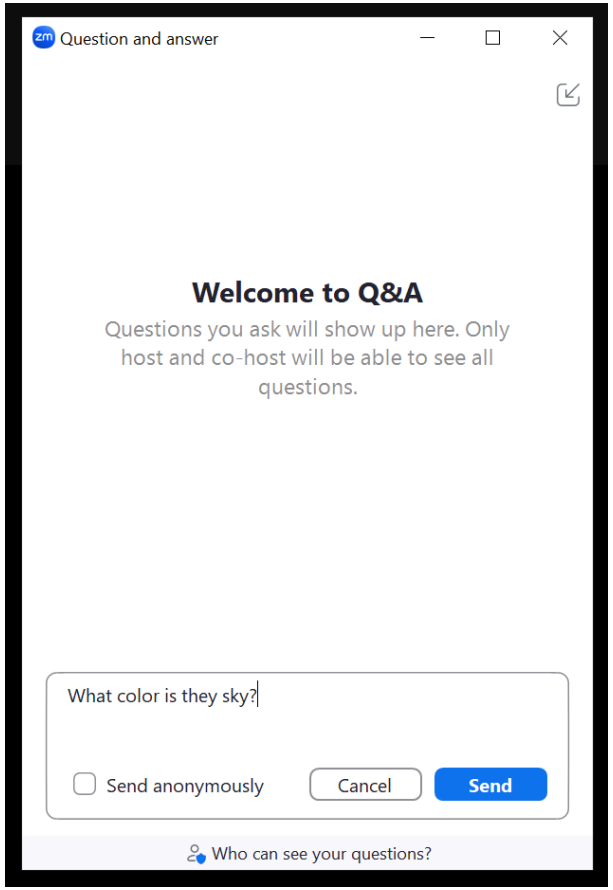
Submitting Questions

Please use the Q&A function to enter your questions.

The project team will review all the questions submitted.



1. To open the Q&A function, click on the “Q&A” icon at the bottom of your screen



2. Type your question in the text box and click Send

Captions

To enable captioning during the event, click on the “Show captions” icon at the bottom of your screen.

NIST National Cybersecurity Center of Excellence

Overview

Cherilyn Pascoe, NCCoE Director

Who We Are

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

A **collaborative hub** convening experts from industry, government, and academia to solve organizations' most pressing cybersecurity challenges

Our Applied Cybersecurity Work

- Demonstrate standards-based, end-to-end solutions using off-the-shelf technology
- Publish usable guides to help U.S. organizations improve their cybersecurity
- Develop risk profiles to help communities prioritize their cybersecurity efforts

Developed collaboratively through 180 agreements with collaborators across vendors, industry, government, and academia

NIST National Cybersecurity Center of Excellence

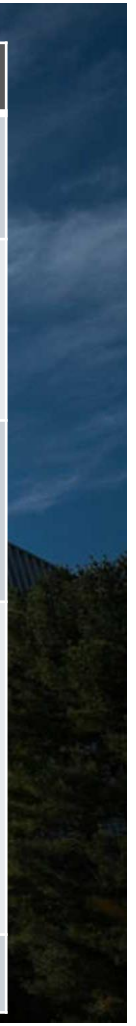
Secure Software Development, Security, and Operations (DevSecOps) Practices

Alper Kerman
Principal Lead
alper.kerman@nist.gov

Virtual Event Agenda

AGENDA

Time (EDT)	Session
1:00 p.m. – 1:05 p.m.	**Welcome** Speaker: **Cherilyn Pascoe, NIST**
1:05 p.m. – 1:30 p.m.	**NCCoE DevSecOps Project Overview** Speaker: **Alper Kerman, NIST** **(Polling questions – Opportunity to provide your feedback)**
1:30 p.m. – 1:50 p.m.	**NIST Secure Software Development Framework (SSDF) Overview** Speaker: **Michael Ogata, NIST** **(Polling questions – Opportunity to provide your feedback)**
1:50 p.m. – 2:35 p.m.	**Panel 1: Cybersecurity Challenges and Recommendations from Software Producers and Consumers** Moderator: **Michael Ogata, NIST** Panelists: **Black Duck (Tim Mackey), DigiCert (Dave Roche), GitLab (MaryGrace Wajda), Microsoft (Tarek Dawoud)** **(Polling questions – Opportunity to provide your feedback)**
2:35 p.m. – 2:40 p.m.	**BREAK**



Virtual Event Agenda

AGENDA

Time (EDT)	Session
2:40 p.m. – 3:25 p.m.	**Panel 2: DevSecOps Use of Artificial Intelligence & Zero Trust** Moderator: **Dr. Parisa Grayeli, NIST/MITRE** Panelists: **CyberArk (Rahul Dubey), Microsoft (Segu Riluvan), NextLabs (Keng Lim), Sagittal AI (Michael Smith), Scribe Security (Daniel Nebenzahl)** **(Polling questions – Opportunity to provide your feedback)**
3:25 p.m. – 3:30 p.m.	**Closing Discussion** Moderator: Alper Kerman, NIST
3:30 p.m.	**Adjourn**

NIST NCCoE DevSecOps Project Team

- **Principal Leads & Point of Contacts**
  - **Alper Kerman** (Alper.Kerman@nist.gov)
  - **Michael Ogata** (Michael.Ogata@nist.gov)


- **Lab SMEs & Engineers**
  - **Dr. Parisa Grayeli** (Parisa.Grayeli@nist.gov)
  - **Phillip Millwee** (Phillip.Millwee@nist.gov)
  - **Allen Tan** (Allen.Tan@nist.gov)



- **Outreach & Engagement**
  - **Tom Walters** (Thomas.Walters@nist.gov)

- **Standards & NIST Special Publication SME Lead**
  - **William Barker** (William.Barker@nist.gov)

Secure Software Development, Security, and Operations (DevSecOps) Practices

OBJECTIVE:

Develop and document an applied risk-based approach and recommendations for secure software development, security, and Operations (DevSecOps) practices consistent with:

- Secure Software Development Framework (SSDF)
- Other NIST, government, and industry guidance

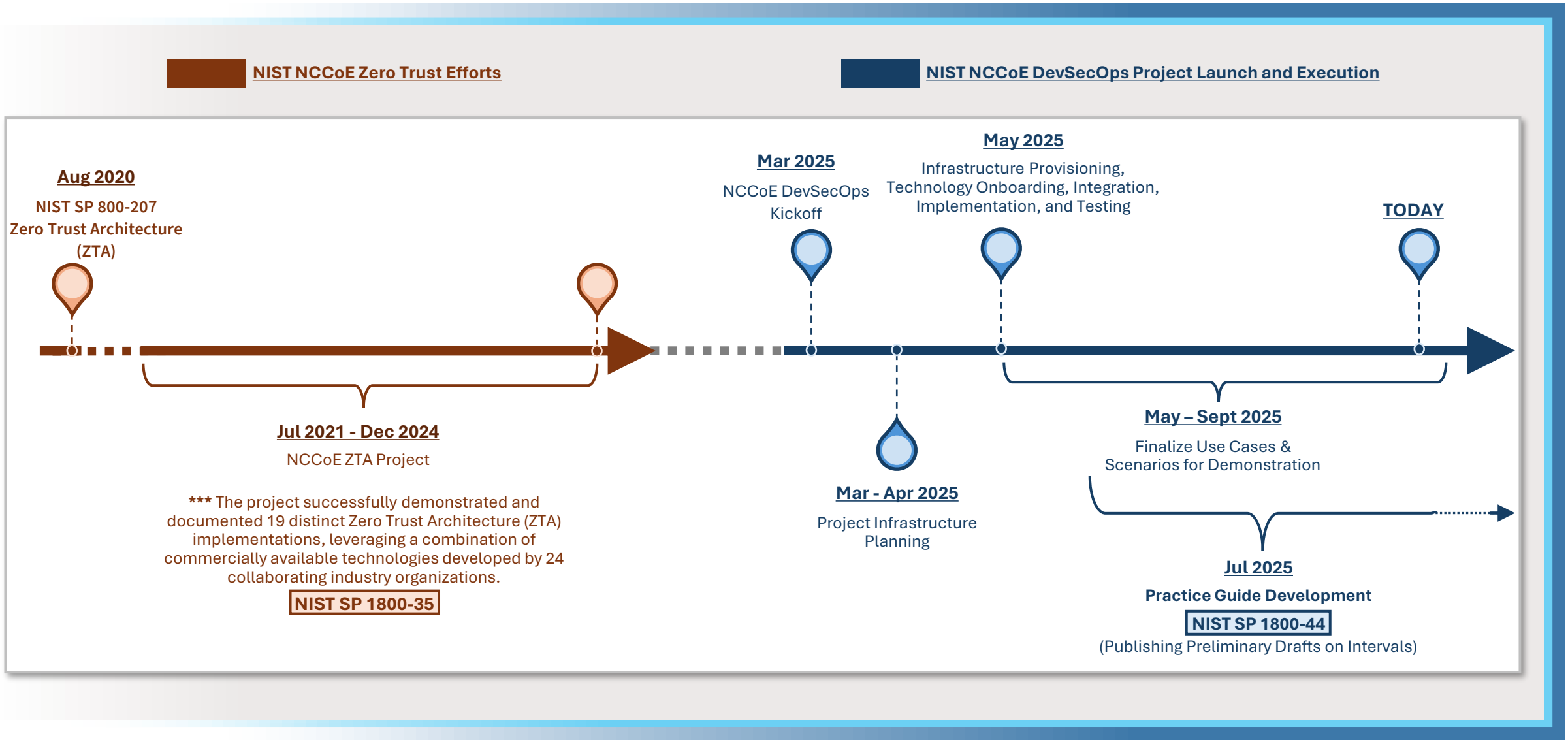
SCENARIOS:

Demonstrate DevSecOps practices in multiple proof-of-concept use case scenarios that involve software development environments integrated with different industry technologies, **including security practices associated with the use of generative AI capabilities and Zero Trust Architectures**.

- **Closed Source Software Development**
- **Free and Open Source Software (FOSS) Development**

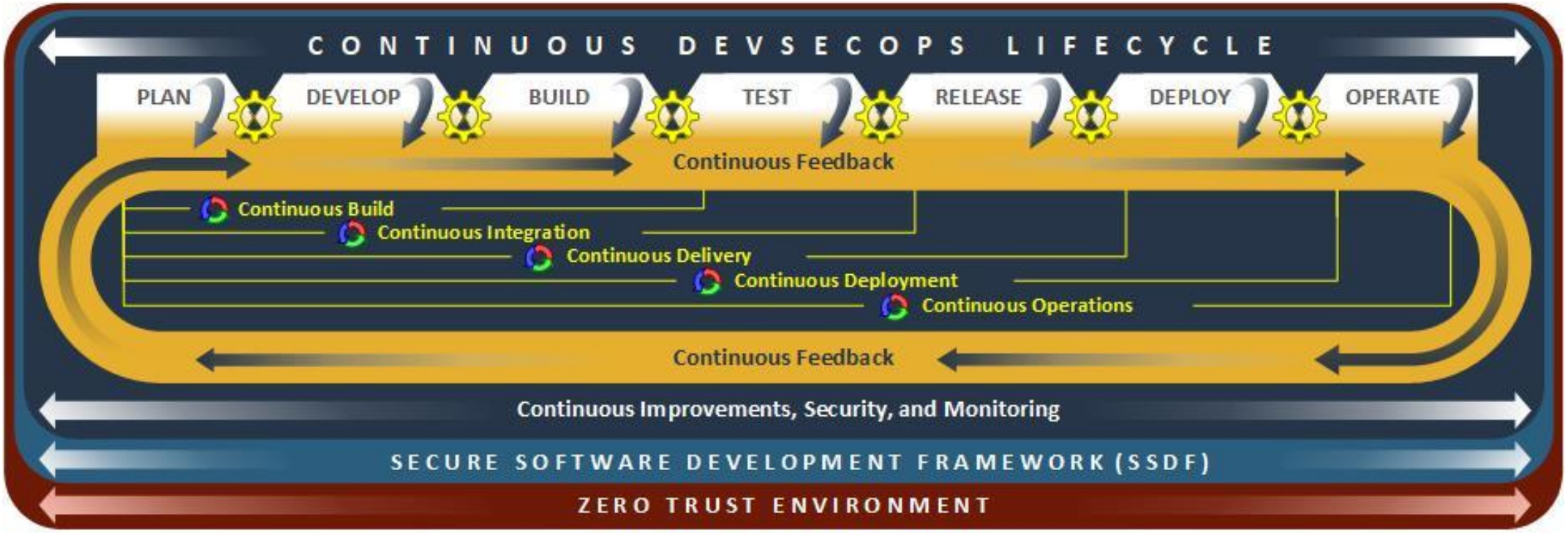
***This project was initiated in March 2025 to support the directive outlined in **Section 2(c)(i) of Executive Order 14306**

NCCoE DevSecOps Project Timeline



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE DevSecOps Project Reference Model



Project's DevSecOps Reference Model – PLAN PHASE

AI Components | DevOps Components | Security Components

AI Components
(e.g., Machine Learning, Generative AI, Chatbots, Agents, Agentic Workflows)

Ticketing System

Functional Requirements Management System

Project Management System
(e.g., Team Planning, Team Collaboration, Training)

Product Management System

Design Management System

Configuration Management System

Security Requirements Management System

Risk Management System

Threat Modeling System

Cyber Intelligence, Threat, and Security Metadata Feeds
(e.g., OpenSSF, NVD, OSV)

Credential Management System

Secrets Management System

Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

Project's DevSecOps Reference Model – DEVELOP PHASE

AI Components | DevOps Components | Security Components

AI Components
(e.g., Machine Learning, Generative AI, Chatbots, Agents, Agentic Workflows)

Client Tool
(e.g., IDE, CLI, Binaries)

Software Libraries
(e.g., Internal and External)

Artifact Repository
(e.g., Internal and External)

Source Code Management (SCM)
(e.g., Version Control, Commit Hooks, Branch/ Merge Protection)

Unit Test Generation

Static Application Security Testing (SAST)

Software Composition Analysis (SCA)

Cyber Intelligence, Threat, and Security Metadata Feeds
(e.g., OpenSSF, NVD, OSV)

Linting

Credential Management System

Secrets Management System

Certificate Management System

Hardware Security Module (HSM) Including Software or Virtual HSM

Firmware Management System

Secret Scanning

Infrastructure as Code (IaC)

Infrastructure as Code (IaC) Scanner

Artifact Signing and Verification
(e.g., Source Code, Commit, Image, Binary, Library)

Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

Project's DevSecOps Reference Model – BUILD PHASE

AI Components | DevOps Components | CI/CD Pipeline | Security Components

AI Components
(e.g., Machine Learning, Generative AI, Chatbots, Agents, Agentic Workflows)

Client Tool
(e.g., CLI, Binaries)

Software Libraries
(e.g., Internal and External)

Artifact Repository
(e.g., Internal and External)

Source Code Management (SCM)
(e.g., Branch/Merge Protection)

Unit Testing

Configuration Management System

Static Application Security Testing (SAST)

Software Composition Analysis (SCA)

Cyber Intelligence, Threat, and Security Metadata Feeds
(e.g., OpenSSF, NVD, OSV)

Linting

Secret Scanning

Infrastructure as Code (IaC)

Infrastructure as Code (IaC) Scanner

Artifact Signing and Verification
(e.g., Image, Binary, Library)

Container Image Scanning

Build Provenance
(e.g., Supply-chain Levels for Software Artifacts (SLSA) Attestation)

Software Bill of Material (SBOM) Generation

Firmware Management System

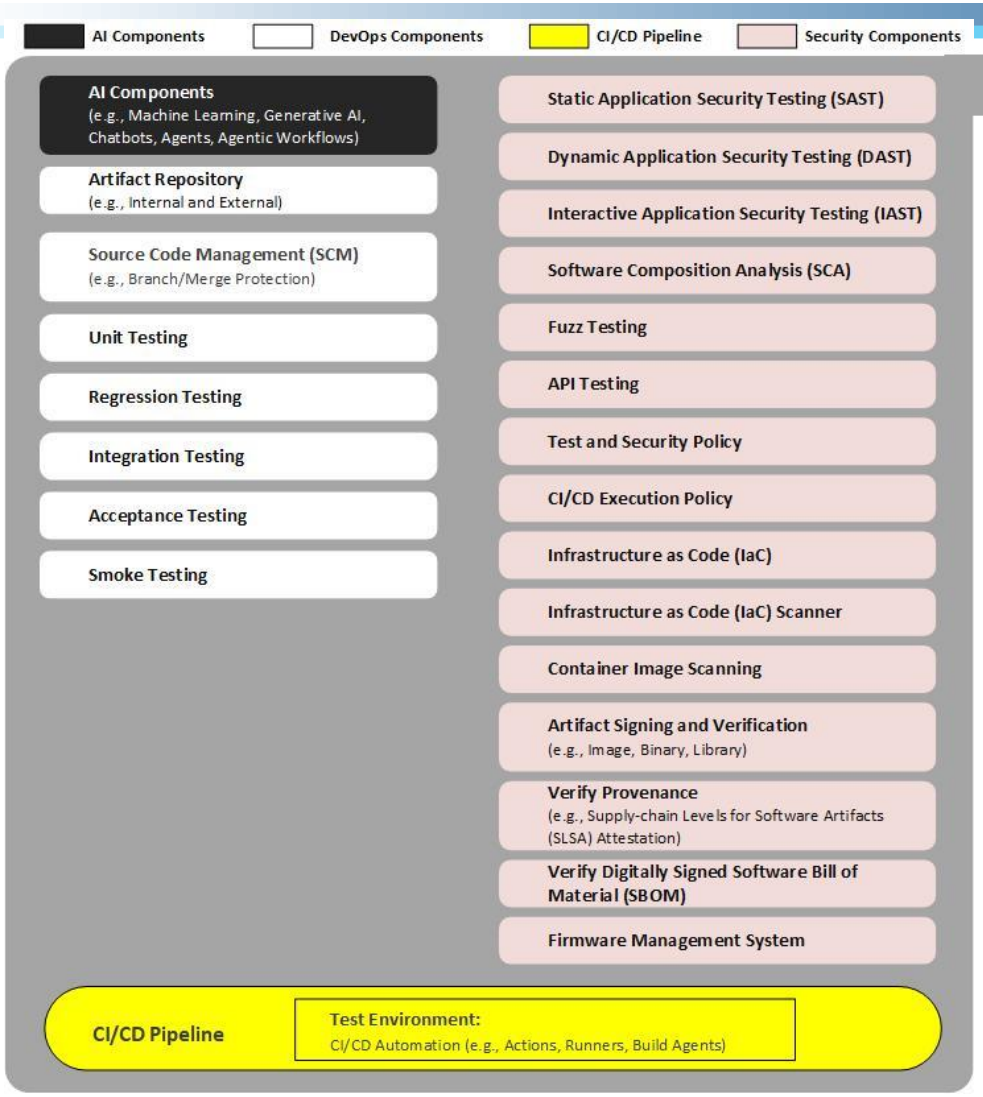
CI/CD Pipeline

Build Environment:
CI/CD Automation (e.g., Actions, Runners, Build Agents)

Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

Project's DevSecOps Reference Model – TEST PHASE



Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

Project's DevSecOps Reference Model – RELEASE PHASE

AI Components | DevOps Components | CI/CD Pipeline | Security Components

- **AI Components** (e.g., Machine Learning, Generative AI, Chatbots, Agents, Agentic Workflows)
- **Artifact Repository** (e.g., Internal and External)
- **Source Code Management (SCM)** (e.g., Branch/Merge Protection)
- **Configuration Management System**
- **Package Management System**
- **Release Management System**
- **Release Evidence**
- **Smoke Testing**
- **Acceptance Testing**
- **Software Composition Analysis (SCA)**
- **Dynamic Application Security Testing (DAST)**
- **Interactive Application Security Testing (IAST)**
- **Artifact Signing and Verification** (e.g., Image, Binary, Library)
- **Container Image Scanning**
- **Infrastructure as Code (IaC)**
- **Infrastructure as Code (IaC) Scanner**
- **Verify Provenance** (e.g., Supply-chain Levels for Software Artifacts (SLSA) Attestation)
- **Verify Digitally Signed Software Bill of Material (SBOM)**
- **Firmware Management System**

CI/CD Pipeline — **Release Environment:** CI/CD Automation (e.g., Actions, Runners, Build Agents)

Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

Project's DevSecOps Reference Model – DEPLOY PHASE

AI Components | DevOps Components | CI/CD Pipeline | Security Components

AI Components
(e.g., Machine Learning, Generative AI, Chatbots, Agents, Agentic Workflows)

Artifact Repository
(e.g., Internal and External)

Configuration Management System

Release Management System

Deployment Management System
(e.g., Release Orchestration, Rollback, Canary)

Infrastructure as Code (IaC)

Infrastructure as Code (IaC) Scanner

Software Bill of Material (SBOM) Management

Artifact Verification
(e.g., Image, Binary, Library)

Firmware Management System

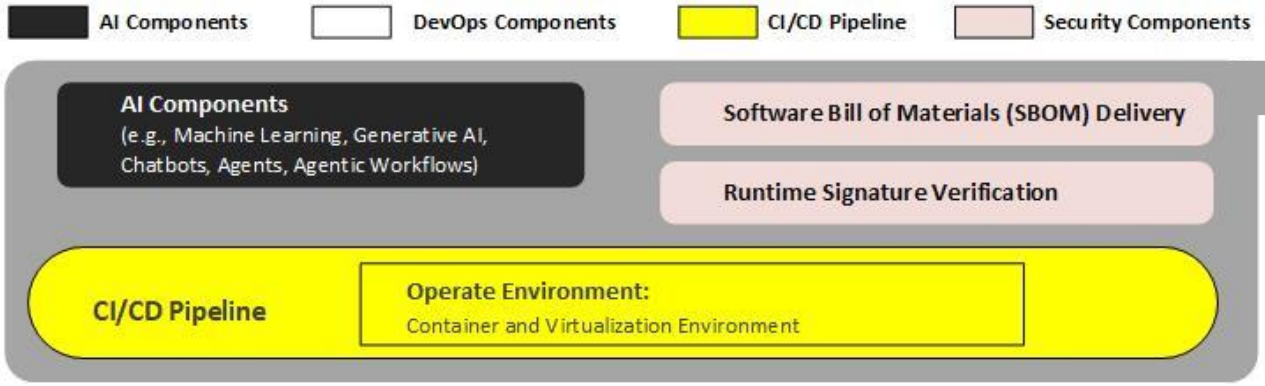
CI/CD Pipeline

Deploy Environment:
Container and Virtualization Environment

Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

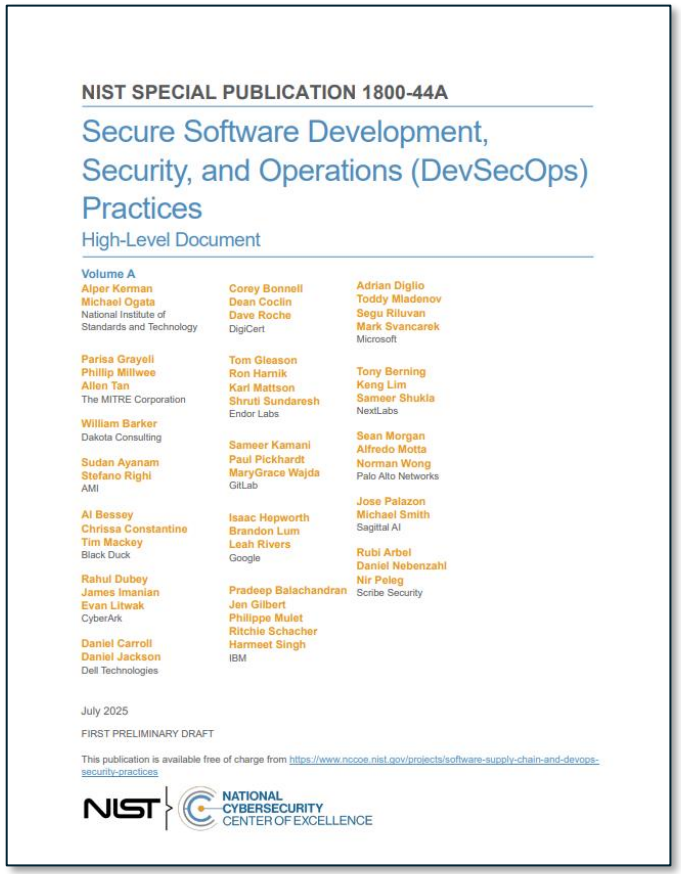
Project's DevSecOps Reference Model – OPERATE PHASE



Applicable Secure Software Development Framework (SSDF, NIST SP - 218 and 218A) Categories:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)

NCCoE DevSecOps Project Output



NIST SPECIAL PUBLICATION 1800-44A

Secure Software Development, Security, and Operations (DevSecOps) Practices

High-Level Document

Volume A

Alper Kerman
Michael Ogata
National Institute of Standards and Technology

Parisa Grayeli
Phillip Millwee
Allen Tan
The MITRE Corporation

William Barker
Dakota Consulting

Sudan Ayanam
Stefano Righi
AMI

Al Bessey
Chrissa Constantine
Tim Mackey
Black Duck

Rahul Dubey
James Imanian
Evan Litwak
CyberArk

Daniel Carroll
Daniel Jackson
Dell Technologies

Corey Bonnell
Dean Coclin
Dave Roche
DigiCert

Tom Gleason
Ron Harnik
Karl Mattson
Shruti Sundaresh
Endor Labs

Sameer Kamani
Paul Pickhardt
MaryGrace Wajda
GitLab

Isaac Hepworth
Brandon Lum
Leah Rivers
Google

Pradeep Balachandran
Jen Gilbert
Philippe Mulet
Ritchie Schacher
Harmeet Singh
IBM

Adrian Diglio
Toddy Mladenov
Segu Riluvan
Mark Svancarek
Microsoft

Tony Berning
Keng Lim
Sameer Shukla
NextLabs

Sean Morgan
Alfredo Motta
Norman Wong
Palo Alto Networks

Jose Palazon
Michael Smith
Sagittal AI

Rubi Arbel
Daniel Nebenzahi
Nir Peleg
Scribe Security

July 2025

FIRST PRELIMINARY DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

***The public comment period for this publication closes on **September 12, 2025**.

NIST Special Publication (SP) 1800-44:

NIST SP 1800-44

- **Version:** First Preliminary Draft (A)
- **Format:** High-Level Document in PDF
- **Date Released:** July 2025, open for public comment until Sept. 12, 2025

- **Next Preliminary Draft Release Date (Tentative):**
  - November 2025

NCCoE DevSecOps Project Collaborators

- AMI
- Black Duck
- CyberArk
- Dell Technologies
- DigiCert
- Endor Labs
- GitLab
- Google
- IBM
- Microsoft
- NextLabs
- Palo Alto Networks
- Sagittal AI
- Scribe Security

Connect with Us

NCCoE DevSecOps Project:

Webpage:

- https://www.nccoe.nist.gov/projects/secure-software-development-security-and-operations-devsecops-practices

Email:

- nccoe-devsecops@list.nist.gov

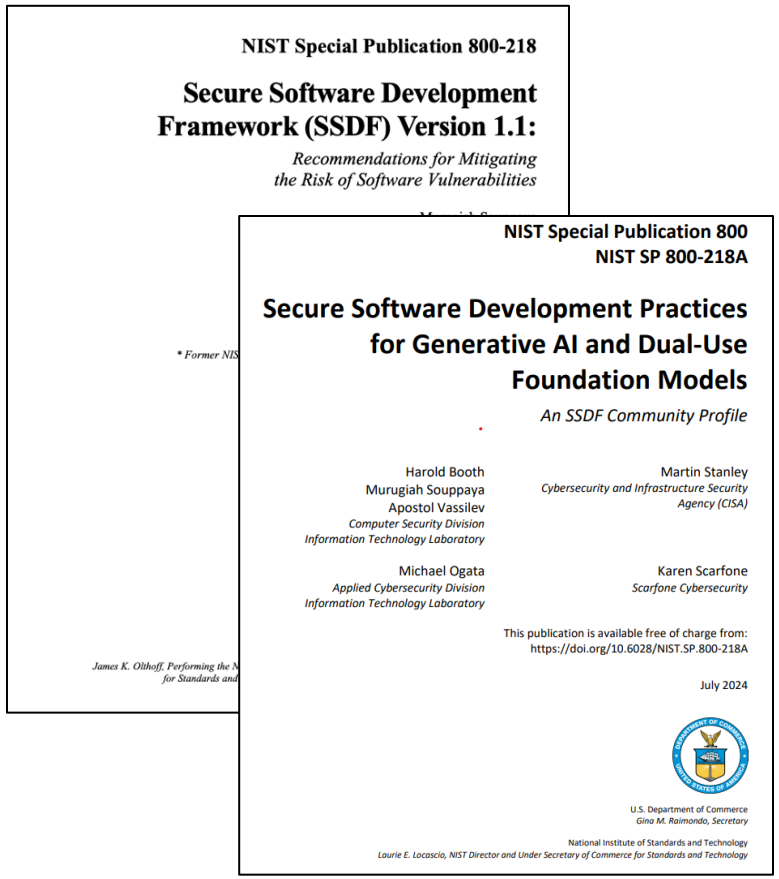
NIST National Cybersecurity Center of Excellence

Secure Software Development Framework (SSDF) Overview

Michael Ogata
Principal Lead
michael.ogata@nist.gov

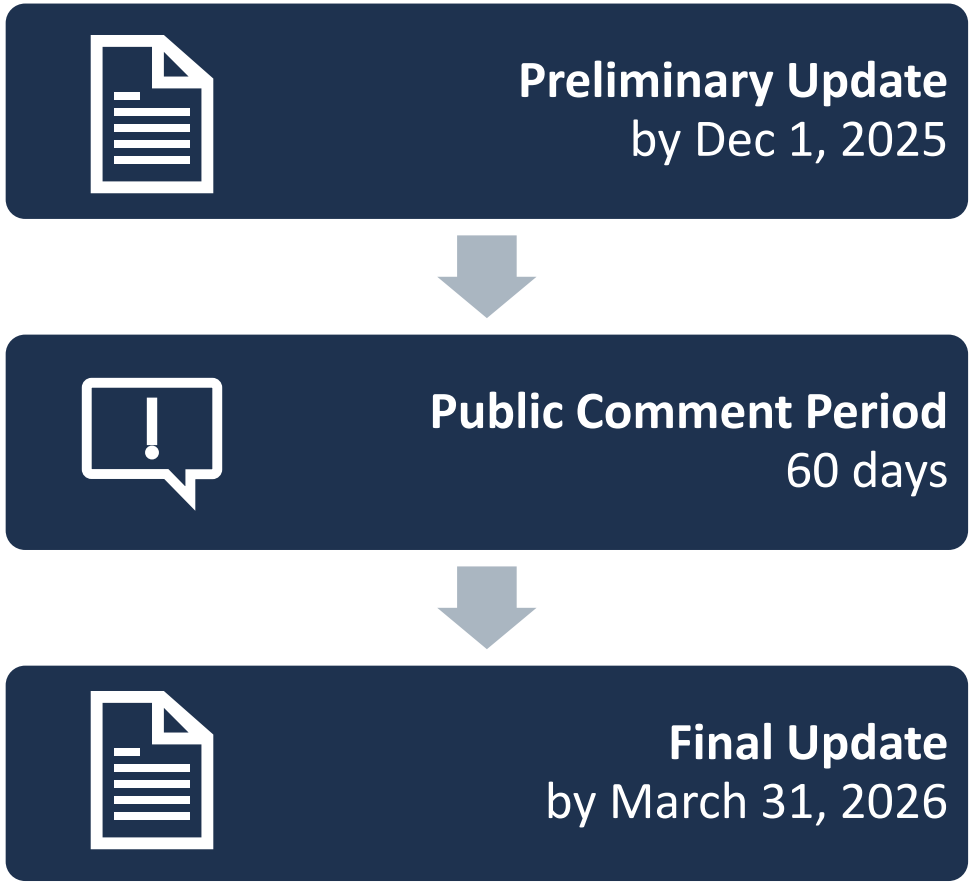
Development Timeline of the SSDF

- **Secure Software Development Framework**
  - **April 2018 -** NIST and SAFECode workshop
  - **June 2019 -** draft white paper
  - **April 2020 -** SSDF V1.0 white paper
  - **September 2021 -** draft SSDF V1.1
  - **February 2022** - final SSDF V1.1
- **Secure Software Development Practices for Generative AI and Dual Use Foundation Models**
  - **April 2024** - NIST SP 800-218A
  - **July 2024** - final NIST SP 800-218A



SSDF Update

- *EO 14306 "update shall include practices, procedures, controls, and implementation examples regarding the secure and reliable development and delivery of software as well as the security of the software itself."*
- Current Proposed feedback includes:
  - Continuous improvement
  - Software updates
  - Additional examples and updated informative references



SSDF Background, Principles, and Architecture

Approach Similar to the Cybersecurity Framework

Provides a common language to describe fundamental, sound secure software development practices

Can help an organization document its secure software development practices today and define its future target practices as part of its continuous improvement process

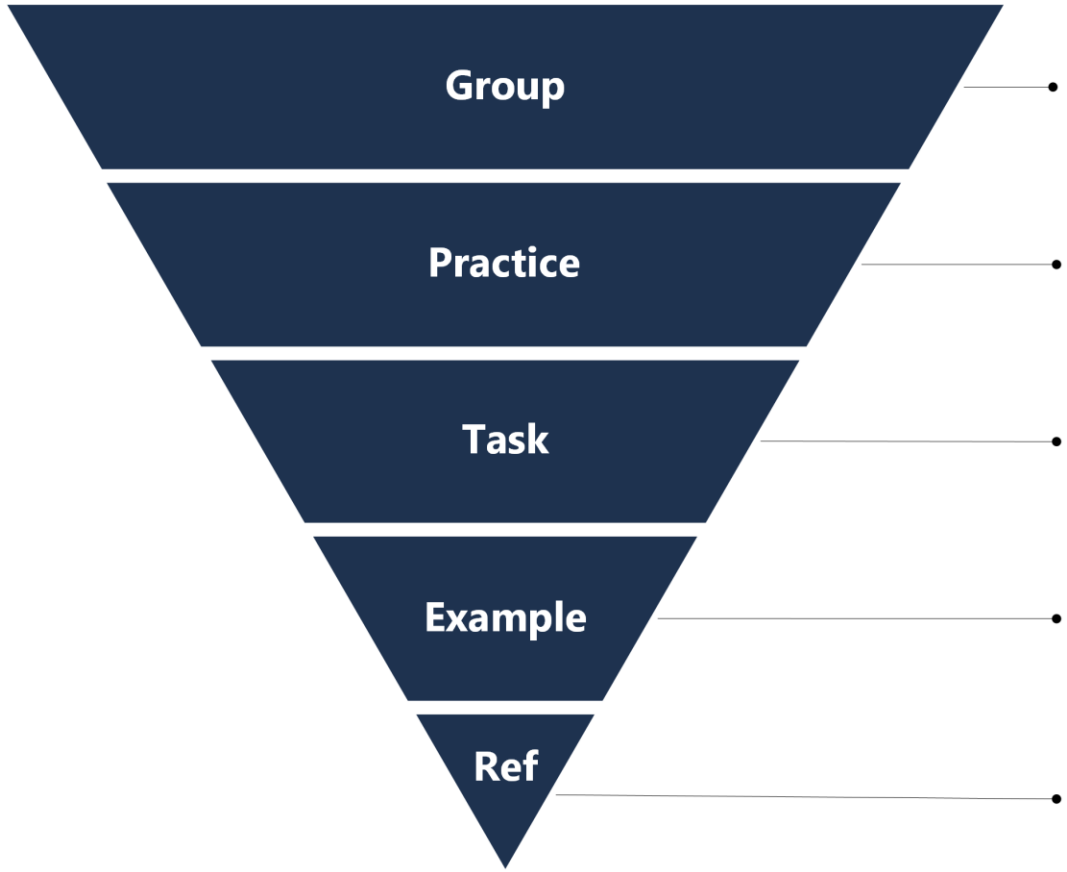
Leverages existing secure software development practices from established standards, guidance, and secure software development practice documents

Do no harm (to organizations who have already adopted established practices)

SSDF Publication Basics

Audience	For both *software producers* (e.g., COTS vendors, government software developers, custom software developers) and *software consumers* (federal government agencies and other organizations)
Flexible	Can be used by organizations in any sector or community, regardless of size or cybersecurity sophistication to manage risks associated with software Can be integrated into any existing software development workflow and automated toolchain
Customizable	Broadly applicable—not specific to technologies e.g., IT, ICS, IoT, or cyber-physical systems (CPS), platforms, programming languages, SDLC models, development environments, operating environments, tools, etc.

SSDF Structure



- A logical collection of practices
- The name of the practice and a unique identifier, followed by a brief explanation of what the practice is and why it is beneficial
- One or more actions that may be needed to perform a practice
- Notional Examples of the types of tools, processes, or other methods that can be used to help implement the task.
- Pointers to one or more established secure development practice documents and their mappings to a particular task.

SSDF Practice Groups

Prepare the Organization (PO): Ensure the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, also for each individual project.

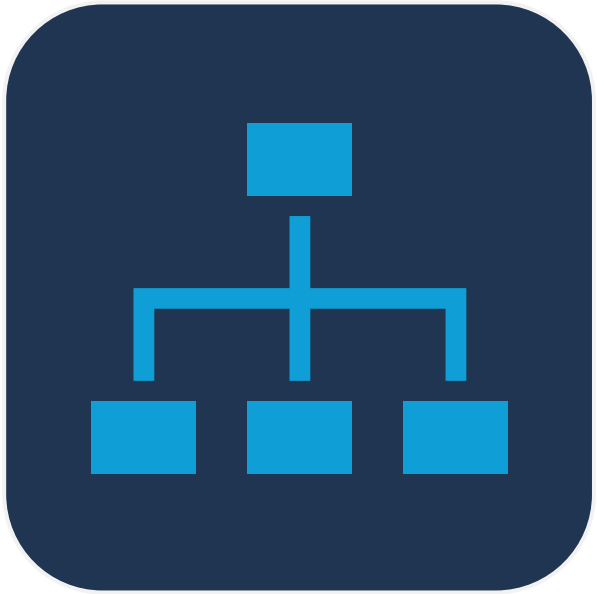
Protect the Software (PS): Protect all components of the software from tampering and unauthorized access.

Produce Well-Secured Software (PW): Produce well-secured software that has minimal security vulnerabilities in its releases.

Respond to Vulnerabilities (RV): Identify vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.

(PO) Prepare the Organization

- (PO.1) Define security requirements for software development
- (PO.2) Implement roles and responsibilities
- (PO.3) Implement supporting toolchains
- (PO.4) Define and use criteria for software security checks
- (PO.5) Implement and maintain secure environments for software development



(PS) Protect the Software

- (PS.1) Protect all forms of code from unauthorized access and tampering
- (PS.2) Provide a mechanism or verifying software release integrity
- (PS.3) Archive and Protect each software release

(PW) Produce Well-Secured Software

- (PW.1) Design software to meet security requirements and mitigate risks
- (PW.2) Review the software design to verify compliance with security requirements
- (PW.3) --
- (PW.4) Reuse existing, well-secured software when feasible instead of duplicating functionality
- (PW.5) Create source code by adhering to secure coding practices
- (PW.6) Configure the compilation. Interpreter, and build processes to improve executable security
- (PW.7) Review and/or analyze human-readable code to identify vulnerabilities and verify compliance with security requirements
- (PW.8) Test executable code to identify vulnerabilities and verify compliance with security requirements
- (PW.9) Configure software to have secure settings by default

(RV) Respond to Vulnerabilities

- (RV.1) Identify and confirm vulnerabilities on an ongoing basis
- (RV.2) Assess, Prioritize, and Remediate vulnerabilities
- (RV.3) Analyze vulnerabilities to identify their root causes

Secure Software Development Practices for Generative AI and Dual-Use Foundation Models

An SSDF Community Profile

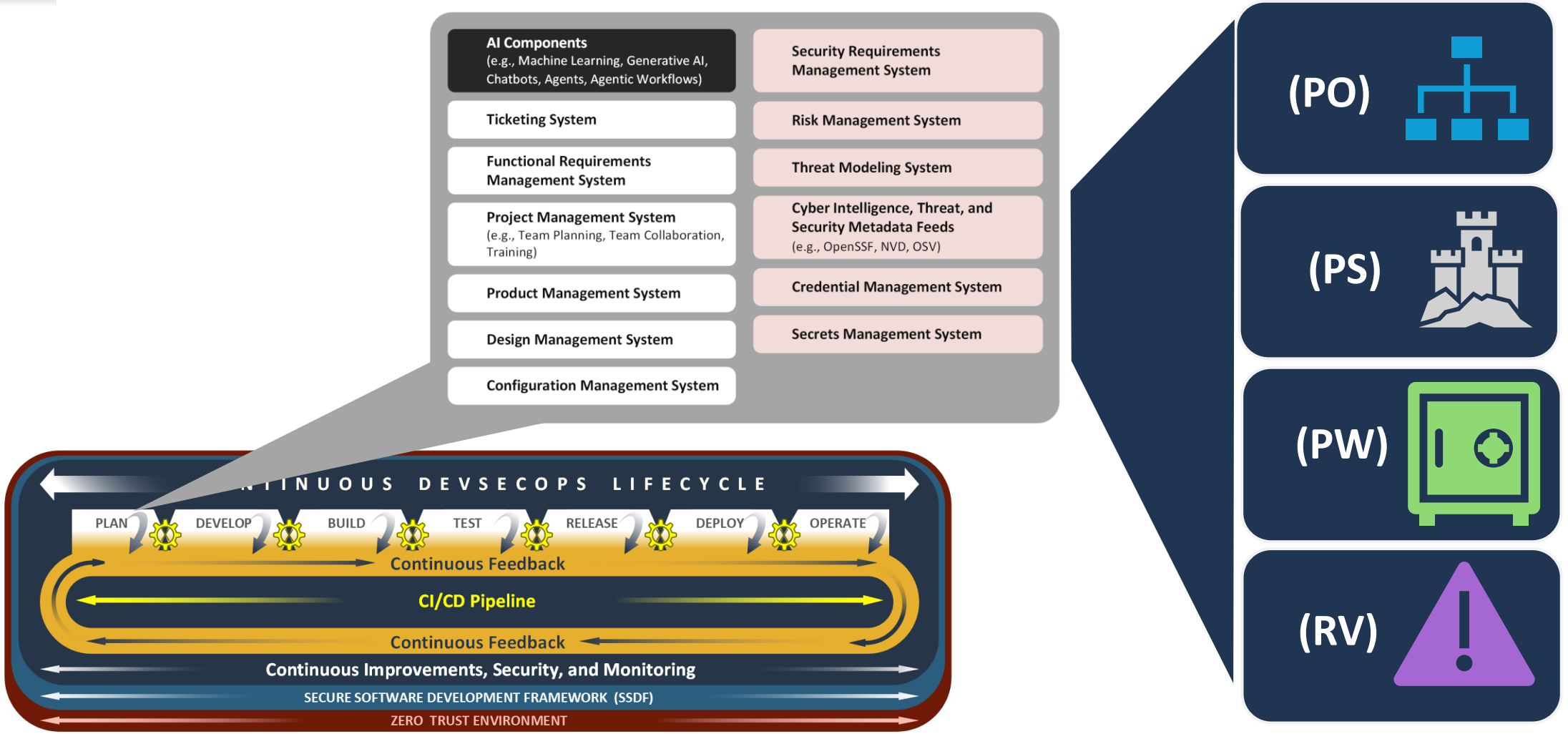
NIST SP 800-218A

- Supplements SSDF v.1.1
- Focuses on AI model development
  - Data sourcing, designing, training, and evaluating AI models
  - Incorporating and integrating AI models into other software
- Tailors existing tasks to be more AI focused
- Augments tasks
  - Priority
  - Recommendations, Considerations, and Notes
  - Targeted AI informative references: *NIST AI 100-1*, *OWASP Top 10 for LLM Applications, etc.*

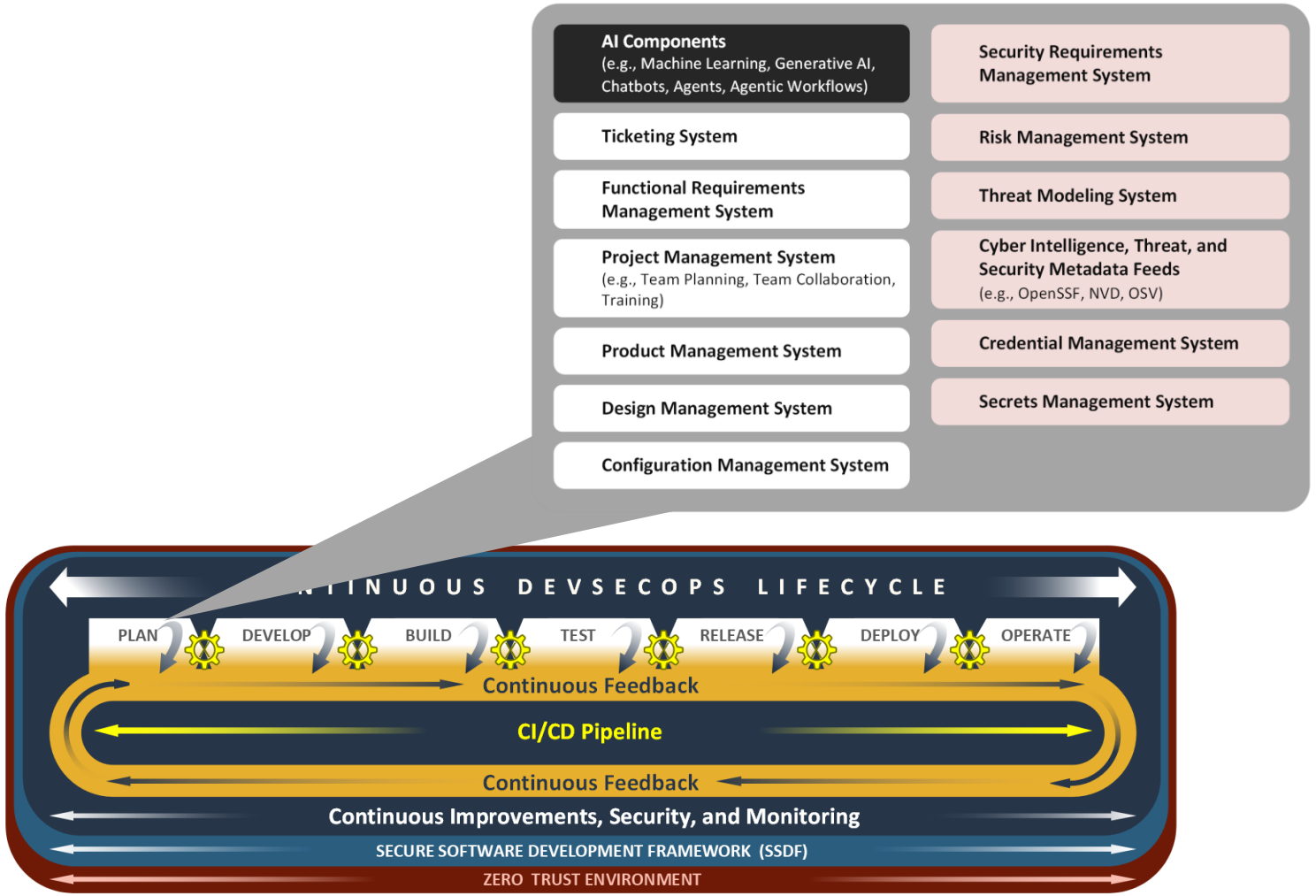
Task	Priority	Recommendations [R], Considerations [C], and Notes [N] Specific to AI Model Development	Informative References
PO.1.1: Identify and document all security requirements for the organization's software development infrastructures and processes, and maintain the requirements	High	**R1:** Include AI model development in the security requirements for software development infrastructure and processes. **R2:** Identify and select appropriate AI model	**AI RMF:** Map 1.3, 1.5, 1.6

The SSDF and the NCCoE DevSecops Project

The SSDF and DevSecOps



The SSDF and DevSecOps



Plan Phase Activity	Description	Components	SP 800-218 Mapping	SP 800-218A Mapping
Team Collaboration	Teams conduct meetings to discuss product design, feature prioritization, task assignments, security vulnerabilities, threats, and software issues.	Project Management System; Ticketing System; Requirements Management System	PO.1.1 PO.1.2 PO.1.3 PO.2.1 PO.2.2 PO.2.3 PW.6.2 PW.7.1 RV.1.1 RV.1.2 RV.2.1 RV.2.2 RV.3.1 RV.3.2	PO.1.1R1 PO1.1R2 PO.1.2R1 PO.1.2N1 PO.1.3R1 PO.2.1R1 PO.2.1N1 PO.4.1R1 PO.4.1C1 PW.7.1R1 PW7.1C1 RV.1.1R2 RV.1.1N1 RV.1.1R3 RV.2.1N1 RV.2.2R1 RV.2.2C1
Functional Requirements Management	Teams identify, document, and prioritize work to implement functional requirements.	Functional Requirements Management System	PO.1.2 PO.2.2 PO.2.3 PO.4.2 PW.1.3 PW.6.2 PW.7.1 PW.8.1 PW.8.2	PO.1.2R1 PO.1.2C1 PO.1.2N1 PO.2.2R1 PO.2.3R1 PO.2.3R1 PO.2.3C1 PO.4.1R1 PW.7.1R1

Panel 1: Cybersecurity Challenges and Recommendations from Software Producers and Consumers

- **Moderator:** Michael Ogata, NIST
- **Panelists:**
  - Black Duck (Tim Mackey)
  - DigiCert (Dave Roche)
  - GitLab (MaryGrace Wajda)
  - Microsoft (Tarek Dawoud)

Break

Panel 2: DevSecOps - Use of Artificial Intelligence and Zero Trust

- **Moderator:** Dr. Parisa Grayeli, NIST/MITRE
- **Panelists:**
  - CyberArk (Rahul Dubey)
  - Microsoft (Segu Riluvan)
  - NextLabs (Keng Lim)
  - Sagittal AI (Michael Smith)
  - Scribe Security (Daniel Nebenzahl)

Putting It All Together

KEY TAKEAWAYS

- **Project objectives:**
  The project's main objective is to demonstrate a risk-based approach to secure software development, security, and operations (DevSecOps) aligned with the NIST Secure Software Development Framework (SSDF).
- **Project focus:**
  The project focuses on Closed Source Software Development Environments in the cloud.
- **Technologies and tools used:**
  The project leverages cutting-edge platforms, technologies, and tools contributed by industry organizations collaborating on the project.
- **Secure use of AI:**
  The project highlights the secure use of AI capabilities.
- **Zero trust principles:**
  The project applies zero trust principles to enhance security postures in DevSecOps environments.
- **SSDF overview:**
  The webinar provided an overview of SSDF, including its purpose, structure, and security practice groups, as well as the tasks within each group.
- **SSDF 218A Community Profile:**
  The webinar covered SSDF 218A Community Profile, which provides guidelines on secure development practices for generative AI and dual-use foundation models.

Project Information:

Webpage:

https://www.nccoe.nist.gov/projects/secure-software-development-security-and-operations-devsecops-practices

For inquiries, email:

nccoe-devsecops@list.nist.gov

***Important Note:** We've gathered all your questions from the webinar and will review and respond to them. The Q&A will be posted on our project's webpage in the coming weeks.

THANK YOU

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE