DEVSECOPS WORKING GROUP CHARTER

Mission Statement

The DevSecOps Working Group is dedicated to advancing modernization across the federal landscape by applying system-level thinking and promoting DevSecOps principles, fostering collaboration through the sharing and implementation of best practices, ensuring secure, efficient, and innovative solutions to support government missions.

Context

The **DevSecOps Working Group** was formed to address software development challenges in the federal sector, focusing on security integration at every phase of the software lifecycle. It promotes cross-functional collaboration between development, security, and operations teams to deliver secure, efficient, and scalable solutions. This security-centric approach, together with continuous learning and automated tools, enhances overall quality throughout the software delivery lifecycle.

Launching a DevSecOps program requires critical attention to change management, workplace culture, and agile methodologies to foster a collaborative environment that supports security without sacrificing speed or innovation. The next evolution will expand automation's role, enhancing feedback loops and increasing lifecycle efficiency.

In times of increasing global uncertainty, the US government must be in position to meet its citizens' needs, maintain superiority in the modern digital landscape and meet emerging threats and is increasingly reliant on the strength of our capabilities and the ability to innovate and modernize our platforms that provide the US with a decisive information advantage.

To achieve this, we must transform government IT components from time and budget vacuums to strategic enablers for mission success. We cannot rely on antiquated tool chains and processes of the past. Our future state of operations depends on our ability to field state-of-the-art resilient software systems rapidly and securely by orders of magnitude faster than we do today.

Scope

The scope of the DevSecOps Working Group includes the following targeted initiatives and collaborative efforts:

1. Framework Development:
    - Create a DevSecOps framework that integrates security throughout all phases of the software lifecycle.
    - Outline a governance model that aligns with federal security standards and regulatory requirements.
2. Solutions Implementation:
    - Develop solutions that enhance mission outcomes and security for federal systems.
    - Address critical considerations to ensure scalable and sustainable DevSecOps practices across federal environments.
3. Cultural Shift:
    - Foster a culture of collaboration between development, security, and operations teams.
    - Enable teams to operate with greater autonomy and agility, promoting strong security practices while reducing dependencies and improving decision-making.

Objective

The objectives of the DevSecOps Working Group are to:

- Develop a practical DevSecOps framework adaptable to federal systems, enhancing collaboration, automation, and the integration of security throughout the software delivery lifecycle.
- Establish a governance model that ensures compliance with federal regulations and security standards, integrating DevSecOps practices seamlessly.
- Enable faster, more reliable software delivery by optimizing processes, reducing bottlenecks, and enhancing overall mission impact.
- Promote cultural change and DevSecOps adoption across all levels, emphasizing executive and leadership buy-in to support a shift towards a DevSecOps-focused mindset and practices throughout the organization.

The group's guiding principles are:

- Solutions-oriented: Focusing on actionable outcomes and practical solutions.
- Positivity: Maintaining a constructive and encouraging environment.
- Problem-solving: Addressing ongoing challenges in federal DevSecOps.
- Forward-thinking: Supporting innovation and continuous improvement.
- Stability and Safety: Ensuring reliable production systems with short feedback loops to maintain security and safety.

Deliverables

The DevSecOps Working Group aims to produce outputs that support the federal adoption of DevSecOps practices:

- DevSecOps Maturity Model Framework: A roadmap for assessing and advancing DevSecOps practices.
- Implementation Patterns: Clear guidelines to assist federal agencies in adopting DevSecOps principles.
- Identification of Success Factors: Curated DevSecOps success factors to ensure robust, secure, and resilient software development.

Deliverables may include various formats, such as white papers, webinars, discussion panels, guest speakers, reference documents, and lab environments. Due to the dynamic nature of DevSecOps, deliverables will be considered 'living documents' and will be subject to periodic review and updates from the working group.

Working Group Membership

Working Group Chairs

Spence Spencer, USPTO, Government Co-Chair
Graham Baggett, US Census Bureau, Government Co-Chair
Susannah Reed, GitLab, Industry Chair
Hasan Yasar, Carnegie Mellon University, FFRDC Chair
Chris O'Neill, Veracode, Industry Vice Chair
Rich Savage, Carahsoft Chair
Kevin Howard, Carahsoft Vice Chair

Working Group Chairs will:

- Attend and contribute to each Working Group meeting
- Prepare the meeting agenda, solicit topics for discussion, assign members to address discussion topics, and distribute meeting materials
- Share information of relevance; provide an update/introduction at the beginning of each meeting to encourage member engagement
- Define and oversee Working Group initiatives and activities
- Assist in all stages of the deliverable production process
- Advocate for government, academic, and industry involvement in the working group
- Referee requests and suggestions for working group membership regarding agenda, deliverables, and representation

Working Group Members

Group members are strictly voluntary, and we strive for a broad representation across government, private sector, and academia.

Working Group Members will:

- Participate in meetings, including exchanging technical information, experiences, and best practices to develop a shared understanding of the topic(s) discussed
- Gather information and work on group deliverables outside of meetings as needed
- Provide feedback on draft deliverables as requested
- Co-lead or participate in Sub-Working Groups (breakout teams/project teams) as needed
- Provide input on meeting agendas as requested

ATARC Support

Elizabeth Wyckoff, Associate Director, Working Groups
Amy Karpowicz, Working Groups Associate
Tim Harvey, Director of Government Engagement

ATARC support will:

- Serve as program management for the Working Group
- Coordinate and drive group projects and deliverables forward
- Schedule Working Group meetings
- Develop Working Group meeting agendas along with the chairs
- Facilitate Working Group meetings along with the chairs
- Assist in distributing relevant documents and materials to Working Group members
- Record meeting minutes, post-meeting decisions, and action items, and distribute them to Working Group members after each meeting
- Assist in preparing final proposals/recommendations
- Provide marketing services for the Working Group (promoting completed deliverables, etc.)
- Develop strategies to improve Working Group engagement, including applicable cross-overs with other Working Groups and relevant events
- Coordinate Working Group Labs as applicable

Rules of Engagement

The Working Group rules of engagement are described as below:

- Meet bi-weekly from 2024 to 2025, or until amended by ATARC Support
- Join Working Group meetings prepared and with requested action items completed
- Provide respectful and constructive feedback to yield the best decisions for the Working Group's objectives
- Endeavour to balance time among members so that all may contribute. All members of the Working Group have a voice and will be listened to.
- Final decisions are made by the Working Group Co-Chairs and ATARC Support
- If a Working Group member misses a meeting, decisions will be made in their absence. The Working Group will consider on a case-by-case basis at the request of the absentee if a decision made in the absence of a member shall be revisited.

The Working Group will:

- Meet every other Wednesday from 2:30-3:30 PM EST.
- Form Sub-Working Groups (breakout teams/project teams) as needed
- Follow the group's ground rules as developed in the charter
- Meet critical deadlines in the creation of deliverables by mutual and balanced effort
- Keep in confidence draft versions of deliverable, off-the-record conversations, and non-public Working Group or ATARC plans to the extent disclosure is not required by law, regulation, or valid court order

File Sharing and Collaboration Tools

Access to the ATARC Box Account is managed by ATARC Support.

Disclaimer: Products and communications by ATARC's DevSecOps Working Group do not necessarily represent the plans or preferences of any company or government agency.