Tuesday, May 6, 2025
11:40 am– 12:00 pm
A Structured Approach to DevSecOps Transformation

Andrew Scherer
IT Transformation Solution Sales Manager, Federal
ServiceNow

Abstract:
For DISA and other DoD organizations, embracing a DevSecOps mindset isn't just a shift in methodology—it's a strategic necessity. The goal is clear: delivering capabilities at the speed of need, supporting the warfighter, and serving a no-fail nation-critical mission. Successful transformation requires a structured approach, balancing agility, security, and operational efficiency.

This journey follows five key steps:

1. Leadership Alignment & Cultural Shift – Secure executive buy-in, foster collaboration, and empower champions.

2. Define a Roadmap & Structure the Transformation – Establish a DevSecOps Center of Excellence (CoE), take a phased approach, and standardize the toolchain.

3. Identify & Prioritize Target Programs for Transition – Use a maturity model to assess readiness and prioritize high-impact applications.

4. Implement Agile Governance & Continuous Improvement – Track performance, measure KPIs, and optimize workflows.

5. Scale & Sustain the Transformation – Embed security into development pipelines, automate compliance, and foster a culture of learning.

The DevSecOps Journey

Leadership:

DISA leadership plays a critical role in driving DevSecOps by aligning initiatives with strategic objectives and ensuring transparency at every stage across teams and domains. A well-defined governance model brings development, security, and operations teams together under a unified framework, breaking down internal silos and fostering collaboration. Identifying DevSecOps champions across teams accelerates adoption, encourages innovation, and creates a structured way to surface and refine new ideas. With leadership commitment and a culture ready for change, the next step is to establish a clear roadmap for execution, setting the foundation for a scalable and sustainable transformation.

Center of Excellence:

A DevSecOps Center of Excellence (CoE) brings together key stakeholders from development, security, IT operations, and compliance to establish policies and governance. Role-based access controls help maintain accountability and security. Taking a phased approach is the most effective strategy—starting with small pilot projects, refining processes based on early results, and expanding as successes build. Standardizing the toolchain is also essential, incorporating CI/CD, security scanning, and automated testing to improve workflows and accelerate software delivery. Meanwhile, agile management practices keep teams aligned, adaptable, and compliant throughout the transformation.

Identify Programs:

Choosing the right programs to transition first is key. A maturity model helps assess readiness and provides a structured way to evaluate potential candidates. Applications with frequent deployments, high change rates, or cloud-native architectures are good starting points, while mission-critical systems benefit from automation to strengthen security and resilience. Enterprise architecture principles help identify application dependencies, address technical debt, and prioritize modernization. A standardized evaluation framework guides decisions by balancing business goals, feasibility, and risk.

Governance:

As DevSecOps takes hold, agile governance and continuous improvement keep teams on track. Objectives and Key Results (OKRs) align efforts with long-term goals, while strategic planning helps teams stay flexible and responsive. Real-time monitoring tracks key metrics like deployment frequency and security compliance, while performance analytics identify bottlenecks and improve efficiency. Continuously measuring outcomes allows teams to refine their approach, strengthening DevSecOps maturity over time.

Scale and Sustain:

Once initial successes are in place, the focus shifts to scaling and sustaining DevSecOps. Repeatable templates and best practices help teams expand adoption across the organization. Security and compliance should be built into development pipelines (Shift Left Security) to catch vulnerabilities early. Automated risk assessments, vulnerability scanning, and real-time threat intelligence strengthen security while reducing operational friction. Visibility into infrastructure, software dependencies, and compliance status keeps governance aligned with DoD requirements.

A strong learning culture is key to long-term success. Ongoing training, knowledge-sharing, and gamification keep teams engaged and drive continuous improvement. By combining automation, best practices, and data-driven insights, organizations can accelerate DevSecOps adoption—delivering secure, high-quality software at mission speed. Starting small, demonstrating quick wins, and scaling strategically will create lasting impact.

Conclusion

This approach empowers DISA and the DoD to achieve a DevSecOps transformation that’s scalable, measurable, and inherently secure. By integrating proven practices with automation and robust governance, organizations can accelerate software delivery, fortify security, and streamline operations—all while adhering to rigorous DoD standards.