

ISSO Support and DevSecOps for the CMS Marketplace

The CMS Marketplace runs FISMA High systems that must ship fast and pass a stack of federal audits. As a subcontractor to the prime, InterSec built DevSecOps into the Expedited Life Cycle and held continuous authority to operate with zero coverage disruptions.

<p>CLIENT Centers for Medicare & Medicaid Services (CMS)</p>	<p>PROFILE Federally Facilitated Exchange; FISMA High healthcare systems</p>	<p>STATUS ● In progress</p>
-----------------------------------------------------------------------------	-----------------------------------------------------------------------------------------	----------------------------------------

<p>9 Years of continuous ISSO support</p>	<p>0 Coverage disruptions from ATO gaps</p>	<p>FISMA High Categorization held throughout</p>	<p>EO 14028 Zero trust and supply chain met</p>
------------------------------------------------------	--------------------------------------------------------	-------------------------------------------------------------	------------------------------------------------------------

<p>ENVIRONMENT FISMA High systems</p>	<p>LIFECYCLE DevSecOps across the XLC</p>	<p>TESTING Continuous penetration testing</p>	<p>AUTHORIZATION Continuous ATO maintained</p>
--------------------------------------------------	------------------------------------------------------	----------------------------------------------------------	-----------------------------------------------------------

— THE CHALLENGE

CMS needed to launch updates rapidly while meeting strict compliance across multiple federal standards. The difficulty came from three directions: multi-layered compliance with cross-agency audits, high-value assets including PII within FISMA High categories, and an Expedited Life Cycle that demanded fast delivery without exposing new vulnerabilities. Speed and assurance had to advance together rather than trade off.

— THE APPROACH

Working as a subcontractor to the prime over roughly nine years, InterSec built DevSecOps checks into each step of the Expedited Life Cycle, so security moved at the same pace as delivery rather than gating it at the end. The approach rested on three practices: apply zero trust and supply chain security, verifying every user and component; run collaborative gate reviews at each milestone; and keep authorization artifacts current so audit readiness was a standing state.

FISMA High and fast release cycles stop being opposites once security lives inside the pipeline.

— THE SOLUTION IN PRACTICE

InterSec combined automated vulnerability scanning with secure coding practices and continuous penetration testing, letting CMS roll out updates with confidence. Ongoing testing and risk assessments caught emergent threats as systems changed. Regular artifact updates kept the program audit-ready and removed last-minute surprises. Application security was built into development, with secure coding standards, automated scans, and code reviews catching vulnerabilities before release.

— RESULTS & IMPACT

- ✓ Continuous authority to operate was maintained, with zero coverage disruptions from authorization gaps.
- ✓ The program met Executive Order 14028 requirements, including zero trust and supply chain security.
- ✓ The security posture improved through DevSecOps practices embedded across the lifecycle.
- ✓ Systems passed annual control assessments and federal audits with minimal findings.

— KEY TAKEAWAYS

Speed and assurance are not a trade-off.

DevSecOps built into the lifecycle lets a high-tempo program ship fast and stay compliant at once.

Continuous ATO is earned by continuous documentation.

Keeping authorization artifacts current turns audit readiness into a standing state.

Audit readiness is a posture, not an event.

Maintaining evidence year-round produces minimal findings across many overlapping audits.

Verify before you trust.

Zero trust and supply chain checks are foundational for high-value federal systems.

CAPABILITIES DEMONSTRATED

ISSO Support (FISMA High)

DevSecOps Across the XLC

Continuous Penetration Testing

Zero Trust and Supply Chain Security

Cross-Agency Audit Readiness

High-tempo delivery and uncompromising compliance can coexist.

InterSec provides ISSO support and DevSecOps for federal programs that cannot slow down or fall out of authorization.

Let's talk →