Executive Summary Two-Page Brief for Leadership

Modernizing Federal Authorization: From Fragmented Compliance to Continuous ATO

Executive Summary for Leadership

The Current State: Fragmented, Costly, and Unsustainable

Today's federal authorization landscape is characterized by duplication, inefficiency, and spiraling costs. Each Program of Record (PoR) operates as an island, making independent technology decisions that compound organizational complexity:

Infrastructure Fragmentation

- Individual programs procure their own hardware, often duplicating capabilities already available elsewhere in the organization
- Each program purchases or builds custom virtual machine infrastructure, creating silos of incompatible systems
- Programs independently acquire or develop secure container runtimes, with no economies of scale or shared security inheritance

Authorization Chaos

- Every ATO package contains one-off requirements unique to that specific system
- No standardized control implementations exist that can be reused across programs
- Each assessment starts from scratch, even when systems share 80%+ of their technical architecture

- Assessors must re-learn each environment rather than building expertise in shared platforms

The True Cost The hidden expense isn't hardware or software—it's labor. Organizations spend millions annually on:

- Redundant documentation efforts across programs
- Manual evidence collection performed separately for each system
- Security engineers context-switching between incompatible environments
- Extended authorization timelines (12-18 months) that delay mission capability
- Continuous re-authorization efforts that consume entire teams

The bottom line: We are paying premium prices for commodity capabilities, and our compliance posture suffers because resources are spread too thin to do anything well.

The Path Forward: Platform-Based Continuous Authorization

Modern DevSecOps practices, combined with a standardized platform approach, fundamentally change this equation. A **DevSecOps Platform (DSOP)** with an approved **secure container runtime** creates a foundation where compliance is inherited, not rebuilt.

Flexible Deployment Options The secure container runtime can be deployed in multiple ways to meet organizational needs:

- **Managed Service** — Centrally-operated platform for organizations wanting turnkey solutions
- **Local Installation** — Self-hosted deployment for programs with dedicated hardware, air-gapped requirements, or specific data residency needs

Both options use the same hardened runtime and inherit the same security controls, ensuring consistent compliance regardless of deployment model.

Shared Infrastructure, Inherited Security Whether centrally-managed or locally-installed, the Kubernetes platform with hardened container runtime provides:

- **One-time platform authorization** that all hosted applications inherit

- Pre-approved base images with embedded security controls
- Standardized network policies, encryption, and access controls
- Continuous monitoring and logging infrastructure shared across all workloads

Automation Replaces Manual Labor With a common platform, compliance automation becomes possible:

- **Machine-readable controls (OSCAL)** that update automatically as configurations change
- **Automated evidence collection** scripts that run continuously, not just before assessments
- **Policy-as-code** enforcement that prevents non-compliant deployments
- **Continuous compliance dashboards** providing real-time authorization status

Standardized Requirements Enable Reuse When all applications deploy to the same platform:

- Control implementations become templates, not one-time documents
- Assessment artifacts are reusable across programs
- Security teams build deep expertise in one environment rather than shallow knowledge of many
- New applications achieve ATO in days or weeks, not months or years

The Continuous ATO (cATO) Model Rather than point-in-time authorization that immediately begins decaying, continuous authorization:

- Maintains real-time visibility into security posture
- Detects and alerts on configuration drift
- Provides ongoing assurance rather than periodic snapshots
- Enables rapid deployment of new capabilities within authorized boundaries

---

Recommendation: Invest in Platform, Harvest the Returns

Summary

CURRENT STATE	FUTURE STATE
Each PoR buys own hardware	Shared, scalable infrastructure
Custom VM/container solutions per program	Single hardened container platform
Unique ATO requirements every time	Standardized, inheritable controls
Manual evidence collection	Automated, continuous compliance
12-18 month authorization cycles	Days-to-weeks for new applications
Millions in duplicated labor	Resources focused on mission, not paperwork

Recommended Actions

1. **Establish a DevSecOps Platform** — Deploy a FedRAMP/DoD-approved Kubernetes environment with hardened container runtime as the standard deployment target for all new applications. Offer both managed service and local installation options to accommodate varying program needs
2. **Pursue Platform-Level Authorization** — Obtain cATO for the platform itself, enabling hosted applications to inherit the majority of security controls
3. **Implement Compliance Automation** — Deploy OSCAL-based documentation, automated evidence collection, and policy-as-code enforcement across the platform
4. **Migrate Existing Workloads** — Prioritize moving current applications to the shared platform, retiring legacy infrastructure and consolidating authorization packages
5. **Measure and Report** — Track authorization timeline reduction, labor cost savings, and security posture improvements to demonstrate ROI

Expected Outcomes

- **80% reduction** in time-to-ATO for new applications
- **Significant cost avoidance** through eliminated hardware/software duplication
- **Improved security posture** via continuous monitoring and standardized controls
- **Faster mission delivery** with security built-in rather than bolted-on
- **Workforce optimization** — security professionals focused on risk, not paperwork

---

The question is not whether we can afford to modernize our authorization approach—it's whether we can afford not to. Every month of delay means more duplicated spending, more manual labor, and more mission capability sitting in authorization queues instead of serving users.

The path forward is clear: shared platforms, inherited controls, automated compliance, continuous authorization.