From Mandate to Mission: Secure Data and AI for Government

Speed through security – doing it right is the cheat code for federal leaders.

OPTIV + ClearShark™

Table of Contents

The Challenge

Mandates vs. Mission Risk

Federal agencies face dual pressures—modernize with AI while staying secure. The fastest path forward starts with cybersecurity shaping your data strategy.

At Optiv + ClearShark, we believe nothing should stand in the way of making government missions more secure. Yet many agencies are stuck in analysis paralysis. They hesitate, fearing compliance gaps or vulnerabilities, while adversaries move ahead with influence campaigns, adaptive attacks, and reconnaissance.

Delaying adoption doesn't keep government safe. Rushing forward without guardrails creates new risks. Agencies need a way to move quickly and responsibly.

The Cheat Code

Five Steps to Mission-Ready AI

You don't need a 200-page playbook. You need a clear path forward. This five-step Cheat Code gives leaders practical guidance to clear obstacles, unblock pilots, and deliver secure, mission-ready outcomes.

Step 1

Data Governance and Taxonomy

Every pilot needs a governance model and taxonomy or it risks stalling.

Solution Roadmap Actions:

- ☐ Assign ownership for data governance.
- ☐ Define a simple taxonomy that separates sensitive from non-sensitive data.
- ☐ Track lineage and provenance before moving data into workflows.

Optiv + ClearShark's **service-first expertise** ensures frameworks are practical and usable.

Step 2

Discovery, Classification and Access

You can't protect what you can't see. Shadow data introduces mission risk.

Solution Roadmap Actions:

- ☐ Build a current catalog with metadata and versions.
- ☐ Classify critical datasets and enforce role-based access.
- ☐ Eliminate untracked data stores that create compliance gaps.

With a **modern data strategy**, agencies catalog and control sensitive data while giving authorized teams the access they need.

Step 3

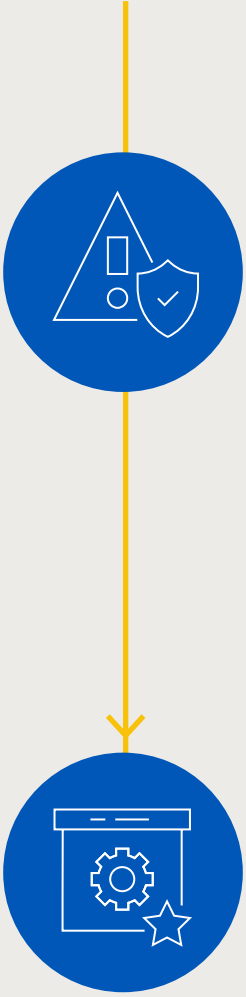
Protection and Monitoring

Not all data carries the same risk. Protect the most sensitive first, then scale.

Solution Roadmap Actions:

- ☐ Identify high-risk datasets such as PII and mission intelligence.
- ☐ Apply encryption at rest and in transit with centralized key management.
- ☐ Monitor continuously for unusual access.

Through **vendor-agnostic frameworks**, Optiv + ClearShark integrates the best protection and monitoring solutions so security grows with the mission.



Step 4

Secure Guardrails for Pilots

Pilots must meet compliance standards from day one. Without guardrails, they create openings for threats.

Solution Roadmap Actions:

- ☐ Launch in hardened, segmented environments.
- ☐ Test through scanning, red teaming and validation.
- ☐ Monitor for drift and misuse during the pilot.

By embedding controls early, Optiv + ClearShark ensures pilots are safe and effective.

Step 5

Use-Case and Model Governance

Not every use case carries the same mission risk. Governance must be risk-tiered, not uniform.

Solution Roadmap Actions:

- ☐ Apply stricter governance to high-value, mission-critical use cases.
- ☐ Track datasets, versions, and labeling workflows for every model.
- ☐ Map governance documentation to ATO requirements from the start

With **proven federal expertise**, Optiv + ClearShark aligns governance with mandates so critical projects move faster without compromise.

The 90-Day Velocity Plan

Once the five steps are in place, this plan keeps momentum going:

Weeks 4–10

Pre-brief

Align leadership, define priorities and set guardrails.

Weeks 4–10

Readiness Assessment

Score governance, infrastructure, and data readiness. Identify gaps.

Weeks 4–10

Pilot

Launch a scoped, ATO-friendly pilot with guardrails in place.
Validate both value and compliance.

Weeks 10–13

Operationalize

Harden for scale, finalize monitoring, and prepare
ATO documentation.

At each stage, leaders can move forward knowing compliance and mission outcomes stay in sync.

From Paralysis to Velocity

Standing still is no longer an option. Without the right partner, speed slows, vulnerabilities grow and missions fall behind.

With Optiv + ClearShark, federal leaders can:

- Turn data into a trusted, strategic asset.
- Adopt securely, responsibly, and at mission speed.
- Balance mandates, compliance and innovation without compromise.

Request your AI Velocity Plan today.

Go from mandate to mission with confidence — and deliver secure, mission-ready outcomes that advance your agency's priorities.

Move fast *because* you're secure.

Appendix: Tools for Federal Leaders

These tools are designed to turn the Five-Step Cheat Code into actionable guidance.
Use them to evaluate readiness, set guardrails, and prioritize what to fix first.

A. Solution Roadmap Checklists

Step 1: Data Governance and Taxonomy

- Do we have a named owner for AI data governance?
- Is there a baseline governance model approved for pilots?
- Have we defined a simple taxonomy to separate sensitive vs. non-sensitive data?
- Is lineage and provenance tracked for datasets feeding AI?
- Are policies documented and repeatable?

Step 2: Discovery, Classification and Access

- Do we have an up-to-date data catalog with metadata and versions?
- Can critical datasets be classified with role-based access?
- Are APIs or integrations in place to allow cross-silo access?
- Do we have visibility into shadow data that may bypass oversight?
- Are access controls auditable and compliant with federal requirements?

Step 3: Protection and Monitoring

- Have we clearly identified high-risk datasets (PII, mission intelligence, etc.)?
- Is encryption enforced at rest and in transit with KMS?
- Do monitoring tools detect anomalous access in real time?
- Are data protection tiers in place?
- Are audit logs maintained and reviewed?

Step 4: Secure Guardrails for Pilots

- Are pilots deployed on hardened VMs or containers with network segmentation?
- Do we conduct validation, adversary testing, and code scanning?
- Is there a process for continuous monitoring during pilots?
- Do pilots align with incident response and compliance frameworks?
- Has leadership approved a guardrails checklist before launch?

Step 5: Use-Case and Model Governance

- Are AI use cases tiered by mission risk with matching controls?
- Do we track datasets, versions, and labeling workflows for each model?
- Is documentation aligned to ATO requirements from the start?
- Are governance artifacts reviewed and updated regularly?
- Is there supply-chain visibility for model provenance?

B. Federal Agency Data and AI Readiness Scorecard

Use this **10-point scorecard** to measure readiness. Each category can be scored 0–10.

1. Data Inventory and Cataloging

- Automated catalog with metadata and lineage (10)
- Partial inventory covering 50–75% (5)
- No systematic cataloging (0)

2. Data Quality and Integrity

- Automated monitoring with <5% error rates (10)
- Basic checks with 5–15% error rates (5)
- No systematic quality checks (0)

3. Data Accessibility and Integration

- Seamless API-driven access across systems (10)
- Partial integration, manual processes (5)
- Data silos, minimal integration (0)

4. Data Governance and Security

- Comprehensive framework with automated compliance monitoring (10)
- Basic policies, manual tracking (5)
- Limited or no governance (0)

5. Data Standardization and Interoperability

- Agency-wide standards and schemas (10)
- Department-level standards, limited alignment (5)
- Inconsistent formats (0)

6. Historical Data Depth and Completeness

- 5+ years of complete mission-critical datasets (10)
- 2–5 years with some gaps (5)
- <2 years or major gaps (0)

7. Real-Time Data Capabilities

- Real-time or near real-time ingestion (10)
- Daily or weekly updates (5)
- Batch processing only (0)

8. Data Privacy and Ethical Compliance

- Automated PII detection and ethical frameworks (10)
- Manual reviews, basic anonymization (5)
- Minimal protections (0)

9. Technical Infrastructure Readiness

- Cloud-native, scalable infrastructure with AI/ML platforms (10)
- Hybrid cloud, partial readiness (5)
- Legacy systems, limited capacity (0)

10. Data Literacy and Workforce Capability

- Dedicated data science teams, agency-wide literacy programs (10)
- Some analytics capability, limited training (5)
- Few skills, no training (0)

Score Interpretation:

90–100: AI Mission Ready

70–89: AI Mission Capable

50–69: AI Mission Developing

30–49: AI Mission Limited

0–29: AI Mission Not Ready

C. Compliance and Risk Notes

Federal frameworks to reference when applying the Cheat Code:

- **FedRAMP** – Cloud system security and monitoring.
- **CMMC** – Maturity model for data protection.
- **ATO (Authority to Operate)** – Required approvals for production systems.
- **OMB AI Memos** – Policy direction for secure adoption.

D. When to Call Experts

Use your readiness score and checklist results to decide:

DIY Quick Wins:

- Build a catalog and taxonomy.
- Encrypt and log critical datasets.
- Run the readiness score quarterly.

Bring in Experts When

- Scaling governance across silos.
- Building an AI-ready data platform.
- Validating models for drift and ATO readiness.
- Hardening infrastructure with adversary testing.

Optiv + ClearShark helps agencies clear roadblocks, align with mandates and deliver mission-ready AI securely.

Want to learn more?

Visit OptivClearShark.com →

7030 Dorsey Road, Suite 102
Hanover, Maryland 21076

info@optivclearshark.com
443.853.1900 | optivclearshark.com

Secure greatness®

©2025 Optiv + ClearShark. All Rights Reserved.
Optiv + ClearShark is a registered trademark
of Optiv Inc.