**AI GOVERNANCE EXECUTIVE GUIDE SERIES • VOLUME 3**

# AI Governance for Federal Programs

*Acquisition, Oversight, and Mission Assurance*

A Practical Guide for OMB M-24-10 Implementation, Contractor AI Oversight, and IG Audit Readiness

**Version 1.0 • December 2025**
Prepared by FERZ LLC
ferz.ai

> *Governance is the authorization boundary: the point where outputs become decisions, and where evidence—not explanations—must exist.*

---

**FOR**

Agency Chief AI Officers • Program Managers • Contracting Officers

Contracting Officer's Representatives • Inspector General Staff • Policy Officers

---

# License and Terms of Use

## Copyright & License

## Commercial Scope Notice

This publication is provided as a public reference framework. Commercial services, tooling, and implementation support derived from this framework are offered separately by FERZ LLC or its authorized partners.

## No Warranty or Endorsement

This document is provided "as is," without warranties of any kind. Use of this framework does not constitute legal or compliance advice.

## Executive At-a-Glance

### Audience

Agency Chief AI Officers, Program Managers, Contracting Officers (COs), Contracting Officer's Representatives (CORs), Inspector General staff, and policy officers responsible for AI systems acquired, developed, or operated under federal contracts.

### Core Thesis

> Governance is the authorization boundary: the point where outputs become decisions, and where evidence—not explanations—must exist.

### Your Challenge

You are responsible for AI systems that contractors build and operate. But contractors often know more about the AI than you do. This creates an accountability gap: you own the risk, but you may lack visibility into the system. This guide helps you close that gap.

### Two Governance Tracks

| Track | Primary Risk | Your Focus |
|---|---|---|
| **Decisioning AI** | Mission risk (safety, rights, security) | Require validation evidence, enforce human oversight |
| **Communications AI** | Records / FOIA exposure | Require records management, disclosure controls |

### Four-Tier Classification

| Tier | Risk Level | What You Require |
|---|---|---|
| Tier 1 | Critical | Full validation evidence, T&E integration, human oversight proof |
| Tier 2 | Elevated | Proportionate validation, annual review, monitoring data |
| Tier 3 | Standard | Operational controls, FedRAMP alignment, basic documentation |
| Tier 4 | Minimal | Acceptable use policy acknowledgment only |

### 90-Day Implementation

- **Weeks 1–4 (Foundation):** Inventory AI across your contracts, establish tiering criteria, draft PWS/SOW clauses
- **Weeks 5–8 (Contractor Oversight):** Require evidence packages from contractors, gap analysis on Tier 1 systems
- **Weeks 9–12 (Operationalization):** Implement monitoring, compile IG-ready documentation, conduct mock audit

# Executive Summary

Federal programs increasingly rely on AI systems that contractors develop, deploy, and operate. You are accountable for these systems—to your agency leadership, to OMB, to your Inspector General, and to the citizens affected by AI-driven decisions. But accountability without visibility is a trap.

The challenge is asymmetric: contractors often understand the AI better than the government program office. They built it. They trained it. They know its limitations. Without the right acquisition structures and oversight mechanisms, you're accepting risk you can't see or manage.

This guide provides the framework to govern AI that contractors operate on your behalf: what to require in contracts, what evidence to demand, how to verify compliance, and how to survive an IG audit.

## The Core Problem: Accountability Without Visibility

OMB M-24-10 makes agencies responsible for AI governance. But when AI is contractor-operated:

- You may not know what AI systems are running on your contracts
- You may not have access to training data, validation results, or performance metrics
- You may learn about problems after they affect citizens or operations
- You bear the accountability, but the contractor holds the information

## The Solution: Governance Through Acquisition

If you can't mandate internally, you can require contractually. This guide provides:

- **PWS/SOW clause templates:** Specific language to include in contracts that requires AI governance
- **Evidence requirements:** What to demand from contractors, scaled by risk tier
- **Verification procedures:** How to confirm contractors are actually complying
- **IG audit preparation:** Documentation that survives Inspector General scrutiny

## Two Governance Tracks

AI governance operates across two distinct tracks with different risks:

| Track | Primary Risk | Key Requirements You Set | Your Oversight Focus |
|---|---|---|---|
| **Decisioning AI** | Rights / safety impact | Validation, bias testing, human oversight | Evidence of testing, approval gates |
| **Communications AI** | Records / FOIA | Federal Records Act compliance, disclosure | Records determination, retention |

**Decisioning AI:** Eligibility determinations, threat detection, resource allocation, predictive analytics that affect mission or citizen outcomes. You must require validation evidence and human oversight mechanisms.

**Communications AI:** Citizen correspondence, caseworker copilots, report drafting, FOIA response assistance. You must require records management controls and clear authorship indication.

While communications AI may not directly execute decisions, its risk can be equal or higher due to Federal Records Act obligations, FOIA exposure, and public trust. Do not assume communications AI is lower risk.

## What This Guide Provides

- **Regulatory foundation:** How OMB M-24-10 and NIST AI RMF translate into contract requirements
- **PWS/SOW clause templates:** Ready-to-use contract language for AI governance
- **Evidence package requirements:** What contractors must provide, by tier
- **Contractor oversight procedures:** How to verify compliance, not just accept assertions
- **IG audit preparation:** Documentation standards and examination playbooks
- **Rights-impacting and safety-impacting AI:** Specific requirements for high-risk categories

# The Regulatory Landscape

## Chapter 1: Your Obligations Under OMB M-24-10

OMB Memorandum M-24-10 establishes AI governance requirements for federal agencies. These requirements apply to AI that contractors operate on your behalf. Understanding your obligations is the foundation for contractor oversight.

### Agency Responsibilities

M-24-10 requires your agency to:

- **Designate a Chief AI Officer:** Accountable for agency AI governance, including contractor-operated AI
- **Maintain an AI inventory:** Including AI systems operated by contractors under federal contracts
- **Implement minimum practices:** For rights-impacting and safety-impacting AI, regardless of who operates it
- **Report annually:** On AI use, including contractor-operated systems

**Key Principle:** Contractor operation does not transfer your accountability. If a contractor operates AI that affects citizens' rights or safety, your agency remains responsible for ensuring it meets OMB requirements.

### Rights-Impacting AI

AI whose outputs serve as a substantial factor in decisions affecting:

- Civil rights, civil liberties, or equal opportunity
- Access to government benefits, services, or programs
- Employment or personnel decisions
- Access to education or housing

For rights-impacting AI, you must require contractors to provide evidence of: impact assessments, bias testing, human oversight mechanisms, notice to affected individuals, and appeal processes.

### Safety-Impacting AI

AI whose outputs serve as a substantial factor in decisions affecting:

- Human life or safety
- Critical infrastructure
- Public health or environment

For safety-impacting AI, you must require contractors to provide evidence of: risk assessments, testing and evaluation, ongoing monitoring, and incident response procedures.

**Agency-Specific Requirements:** OMB M-24-10 establishes minimum requirements. Individual agencies (DoD, DHS, HHS, VA, and others) may impose stricter controls through agency-specific AI policies, directives, or guidance. Always check for agency supplements that may exceed M-24-10 minimums.

### NIST AI Risk Management Framework

While voluntary, NIST AI RMF provides the operational structure for meeting OMB requirements. Require contractors to demonstrate alignment with:

- **GOVERN:** Policies, roles, accountability structures for AI risk management
- **MAP:** Documentation of AI system context, capabilities, and limitations
- **MEASURE:** Methods for assessing and tracking AI risks
- **MANAGE:** Procedures for responding to and mitigating AI risks

# Chapter 2: The Contractor Oversight Challenge

Government IT is largely outsourced. This creates structural challenges for AI governance that you must address through acquisition and oversight.

## The Information Asymmetry Problem

Contractors typically have advantages you don't:

- **Technical depth:** They built the AI. They understand its architecture, training data, and failure modes.
- **Operational visibility:** They see performance data daily. You may see quarterly reports.
- **Incentive alignment:** Their incentive is to deliver on contract terms. Transparency about AI limitations may not serve that goal.

## The Authority Fragmentation Problem

Your governance authority is often fragmented:

- **CO authority:** Can modify contracts, but may lack technical AI expertise
- **COR authority:** Monitors performance, but may lack authority to require changes
- **Program office:** Understands mission, but may not control procurement
- **Agency CAIO:** Has AI governance mandate, but may lack contract-level enforcement

## The Solution: Governance Through Acquisition

You can't mandate what's not in the contract. But you can:

- Include AI governance requirements in new contracts from the start
- Modify existing contracts to add AI oversight provisions
- Require evidence packages as contract deliverables
- Make AI governance compliance a factor in performance evaluation
- Exercise audit rights to verify contractor assertions

## What Contractors Don't Want to Provide (But You Should Require)

Contractors may resist providing:

- **Training data demographics:** Reveals potential bias issues
- **Validation results by subgroup:** May show disparate performance
- **Incident history:** Reveals past problems
- **Limitation documentation:** Undermines marketing claims
- **Audit access:** Enables independent verification

Resistance to providing these items is itself a signal. Make them contractual requirements.

# Risk Framework

## Chapter 3: AI System Classification

### What Counts as AI Under Your Contracts

Contractors may not volunteer that a system includes AI. You must define AI broadly in contracts:

- **Include:** Machine learning models, neural networks, expert systems, automated decision systems, predictive analytics, natural language processing, computer vision, robotic process automation with adaptive logic.
- **Include embedded AI:** AI features within commercial products (e.g., cloud platform AI services, productivity tool copilots, search with AI ranking).
- **Include subcontractor AI:** AI provided by subcontractors as part of prime contractor performance.

### The Four-Tier Framework

Not all AI requires the same oversight. Use this framework to calibrate your requirements:

| Tier | Criteria | Examples | What You Require |
|------|----------|----------|------------------|
| Tier 1 | Rights-impacting, safety-impacting, mission-critical | Benefits eligibility, threat detection, autonomous systems, citizen triage | Full evidence package, T&E results, bias testing, human oversight proof, incident history |
| Tier 2 | Operational impact, federal employee-facing, significant data | Caseworker tools, procurement assist, document processing | Validation summary, annual review, monitoring data, access for verification |
| Tier 3 | Internal operations, no citizen impact, low sensitivity | Meeting transcription, internal search, scheduling | Basic documentation, security controls, acceptable use compliance |
| Tier 4 | Personal productivity, no government data | General research tools, personal drafting | Acceptable use policy only |

### Automatic Tier 1 Triggers

Contractors may try to classify AI as lower-tier to avoid oversight. These conditions automatically trigger Tier 1 requirements, regardless of contractor assertions:

**AUTOMATIC TIER 1 TRIGGERS — Non-Negotiable**

1. Rights-impacting: Outputs substantially factor into decisions affecting civil rights, civil liberties, or equal opportunity
2. Safety-impacting: Outputs substantially factor into decisions affecting human life, safety, or critical infrastructure
3. Produces citizen-facing determinations (even if contractor claims "human reviewed")
4. Involves classified, CUI, or sensitive PII in decision logic
5. Has autonomous or semi-autonomous action capability

# Chapter 4: Contractor Evidence Requirements

You can't verify what you don't require. This chapter specifies what evidence to demand from contractors, by tier.

## Tier 1 Evidence Package

For every Tier 1 AI system, require contractors to provide:

| Evidence Item | What It Contains | Why You Need It |
|---|---|---|
| AI System Description | Architecture, intended use, decision authority, limitations, contraindications | Establishes scope and boundaries of the system |
| Training Data Documentation | Sources, demographics, selection criteria, known gaps, provenance chain | Enables assessment of bias risk and representativeness |
| Validation Results | Performance metrics, demographic subgroup analysis, false positive/negative rates | Proves the system works as claimed, across populations |
| Bias/Fairness Testing | Testing methodology, results by protected class proxies, remediation steps | Required for rights-impacting AI; surfaces disparate impact |
| Human Oversight Procedures | Who reviews, with what authority, what training, escalation paths | Proves "human in the loop" is meaningful, not checkbox |
| Incident History | Past failures, complaints, near-misses, corrective actions taken | Reveals problems contractor may not volunteer |
| Monitoring Procedures | What metrics, how often, drift detection, alert thresholds | Ensures ongoing performance, not just initial validation |

## Tier 2 Evidence Package

For Tier 2 AI systems, require:

- AI system description and intended use statement
- Validation summary (may be less detailed than Tier 1)
- Annual performance review results
- Monitoring data (quarterly)
- Access for government verification

## Tier 3 Evidence Package

- AI system description
- Security and data handling documentation
- Acceptable use policy compliance attestation

## What "Human Oversight" Actually Means

Contractors often claim "human in the loop" without meaningful review. Require contractors to demonstrate:

- **Authority:** The human reviewer has authority to override or block the AI output
- **Training:** Reviewers are trained on AI limitations and what to look for
- **Time:** Reviewers have adequate time to actually review (not just click "approve")
- **Accountability:** Reviewers are accountable for decisions they approve

Checkbox acknowledgments without substantive review do not satisfy human oversight requirements.

# Acquisition Integration

## Chapter 5: PWS/SOW Clause Templates

These clauses should be included in Performance Work Statements and Statements of Work. They flow AI governance requirements to contractors and establish your oversight rights.

### AI System Definition Clause

Include in every contract to establish scope:

**H.XX  AI SYSTEM DEFINITION**

(a) "AI System" means any software that uses machine learning, neural networks, natural language processing, computer vision, or other techniques to generate outputs, predictions, recommendations, or decisions that would otherwise require human judgment—including statistical, algorithmic, or rule-based decision systems that materially influence outcomes. This includes:

(1) Standalone AI tools and platforms;

(2) AI features embedded within commercial products;

(3) AI services accessed via API or cloud;

(4) AI systems provided by subcontractors.

(b) "Governed Unit" means an AI System performing a defined use case within a business process, including its inputs, outputs, integrations, and decision authority. The same AI System deployed in different use cases constitutes separate Governed Units, each subject to independent classification and governance.

(c) The Contractor shall notify the Contracting Officer of any AI System used in performance of this contract within 30 days of first use, and shall identify each distinct Governed Unit.

### AI Inventory and Classification Clause

**H.XX  AI INVENTORY AND CLASSIFICATION**

(a) The Contractor shall maintain a complete inventory of all AI Systems used in contract performance, including systems provided by subcontractors.

(b) For each AI System, the Contractor shall provide to the Contracting Officer:

(1) System name and description;

(2) Intended use and decision authority;

(3) Data types processed;

(4) Proposed risk tier classification with justification;

(5) Whether the system is rights-impacting or safety-impacting.

(c) The Government reserves the right to reclassify any AI System to a higher tier.

### Tier 1 AI Governance Requirements Clause

**H.XX  TIER 1 AI GOVERNANCE REQUIREMENTS**

(a) For any AI System classified as Tier 1 (rights-impacting, safety-impacting, or mission-critical), the Contractor shall provide:

(1) Training data documentation including sources, demographics, selection criteria, and known limitations;

(2) Validation results including performance metrics across demographic subgroups;

(3) Bias and fairness testing methodology and results;

(4) Human oversight procedures demonstrating meaningful review capability;

(5) Incident history and corrective actions;

(6) Ongoing monitoring procedures and performance data.

(b) The Contractor shall obtain Contracting Officer approval before deploying any Tier 1 AI System.

(c) The Contractor shall notify the Contracting Officer within 48 hours of any incident affecting Tier 1 AI System performance or citizen outcomes.

## AI System Suspension Clause (Optional — Tier 1)

For mission-critical or safety-impacting AI, consider including this suspension authority:

**H.XX  AI SYSTEM SUSPENSION AUTHORITY**

(a) The Government may direct the Contractor to suspend operation of any AI System, in whole or in part, pending investigation of:

(1) Reported or suspected incidents affecting citizen outcomes or mission performance;

(2) Evidence of bias, discrimination, or disparate impact;

(3) Material deviation from validated performance parameters;

(4) Failure to provide required documentation or access.

(b) The Contractor shall suspend AI System operation within 24 hours of Government direction and shall not resume operation without written Contracting Officer authorization.

(c) Suspension under this clause does not constitute a termination for convenience or default.

## AI Audit Rights Clause

**H.XX  AI AUDIT AND INSPECTION RIGHTS**

(a) The Government, including the Inspector General, reserves the right to audit, inspect, and test any AI System used in contract performance. This includes access to:

(1) AI system documentation, training data descriptions, and validation records;

(2) Performance monitoring data and incident logs;

(3) Personnel involved in AI development and operation for interview;

(4) Test environments for independent validation.

(b) The Contractor shall provide requested AI documentation within 5 business days of Government request.

(c) The Contractor shall flow down equivalent audit rights to subcontractors providing AI Systems.

## AI Subcontractor Flow-Down Clause

**H.XX  AI GOVERNANCE FLOW-DOWN**

(a) The Contractor shall flow down all AI governance requirements to subcontractors providing AI Systems or AI-enabled services.

(b) The Contractor is responsible for subcontractor AI governance compliance and shall maintain evidence of compliance available for Government inspection.

(c) The Contractor shall notify the Contracting Officer within 48 hours of any subcontractor AI System incident.

(d) The Government may require direct access to subcontractor AI documentation and personnel.

## GenAI-Specific Controls Clause

**H.XX  GENERATIVE AI CONTROLS**

(a) For any generative AI used in contract performance, the Contractor shall:

(1) Prevent input of classified, CUI, or sensitive PII without appropriate controls;

(2) Require human review of AI-generated content before external release or entry into federal records;

(3) Clearly indicate when content is AI-generated in any document that becomes a federal record;

(4) Retain AI-generated drafts as well as final versions in accordance with applicable NARA General Records Schedules and agency-specific records schedules.

(b) The Contractor shall not use generative AI for autonomous citizen-facing communications without explicit Contracting Officer approval.

# Oversight and Verification

## Chapter 6: Verifying Contractor Compliance

Requiring evidence is not enough. You must verify that contractors are actually complying, not just providing paperwork.

### Verification Activities by Tier

| Activity | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|
| Review evidence package for completeness | Before deployment | Before deployment | Annual |
| Validate contractor tier classification | Before deployment | Before deployment | As needed |
| Spot-check performance monitoring data | Quarterly | Semi-annual | N/A |
| Independent testing (sample cases) | Annual | As needed | N/A |
| Interview contractor AI personnel | Before deployment + annual | As needed | N/A |
| Review incident reports and corrective actions | Within 72 hours of incident | Monthly | N/A |

### Red Flags That Require Escalation

Escalate to your CO, agency CAIO, or IG if you observe:

- Contractor unable to produce required documentation within specified timeframe
- Evidence package contains obvious gaps or inconsistencies
- Contractor resists or delays audit/inspection requests
- Performance monitoring data shows unexplained degradation
- Incidents not reported within required timeframes
- Contractor claims AI is "proprietary" to avoid providing documentation
- Tier classification appears inconsistent with actual system risk

### When to Conduct Independent Testing

Don't rely solely on contractor-provided validation. Conduct independent testing when:

- Deploying a new Tier 1 AI system
- Contractor validation methodology appears weak
- User complaints suggest performance issues
- IG or GAO audit is anticipated
- Significant changes to AI system are deployed

# Chapter 7: IG Audit Readiness

Your Inspector General is increasing focus on AI. This chapter helps you prepare for and survive AI-related audits.

## What IG Will Ask For

Based on emerging IG audit practices, expect requests for:

### Inventory and Governance

- Complete inventory of AI systems on your contracts
- Evidence of risk tiering and classification rationale
- Policies and procedures for AI oversight
- Roles and responsibilities for AI governance

### Contractor Oversight

- Evidence that you required AI governance in contracts
- Evidence packages received from contractors
- Records of your verification activities
- Incident reports and your response

### Compliance with OMB M-24-10

- How you identified rights-impacting and safety-impacting AI
- Evidence that minimum practices are in place for high-risk AI
- Coordination with agency CAIO

## Building Your IG-Ready Documentation

For each Tier 1 AI system, maintain a ready-reference file containing:

| Tab | Contents |
|---|---|
| 1 | Contract excerpt showing AI governance clauses you included |
| 2 | AI inventory entry with tier classification and your rationale |
| 3 | Contractor evidence package (complete) |
| 4 | Your verification activities and findings |
| 5 | Incident reports and corrective actions |
| 6 | Your approval decision and sign-off for deployment |

## Common IG Findings to Avoid

IG audits frequently find:

- **No AI inventory:** You didn't know what AI was running on your contracts
- **Incomplete contracts:** AI governance requirements weren't in the PWS/SOW
- **Missing evidence:** You couldn't produce contractor documentation
- **No verification:** You accepted contractor assertions without checking
- **Tier shopping:** High-risk AI was classified as low-tier to avoid oversight
- **Incident gaps:** You didn't know about AI problems until the audit

This guide helps you avoid each of these findings.

# Governance Structure

## Chapter 8: Organizational Model

Effective AI governance requires clear roles, authority, and coordination across your organization.

### Key Roles and Responsibilities

| Role | AI Governance Responsibilities |
|---|---|
| **Agency Chief AI Officer** | Enterprise AI policy, OMB reporting, agency-wide inventory, coordination across programs |
| **Program Manager** | AI oversight for program contracts, tier classification, evidence review, verification activities |
| **Contracting Officer** | Include AI clauses in contracts, approve modifications, enforce contract AI requirements |
| **COR** | Day-to-day contractor oversight, evidence collection, verification, incident monitoring |
| **IG Liaison** | Audit preparation, documentation maintenance, IG coordination |

### Governance Authority Requirements

AI governance fails when the oversight function lacks authority or competence. Ensure:

#### Authority Requirements

- **Contract leverage:** AI governance must be in the contract. CO must be willing to include and enforce AI clauses.
- **Tier determination authority:** Government, not contractor, has final authority on tier classification.
- **Approval gates:** Tier 1 AI cannot deploy without your explicit approval.
- **Escalation path:** Clear path to stop contractor AI deployment when governance is inadequate.

#### Competence Requirements

- **Understand AI basics:** Program staff must understand enough AI to evaluate contractor claims.
- **Know your contracts:** Know what AI governance requirements are in your contracts.
- **Access expertise:** Have access to technical AI expertise for complex validation.

### Coordination with Agency CAIO

Your program-level AI governance should coordinate with agency-level governance:

- Report AI inventory to agency CAIO office
- Align tier classifications with agency standards
- Escalate novel or high-risk AI for agency review
- Participate in agency AI governance working groups

# Implementation Roadmap

## Chapter 9: 90-Day Implementation Plan

### Phase 1: Foundation (Weeks 1-4)

#### Week 1-2: Inventory and Assessment

- Identify all contracts that may involve AI
- Request AI inventory from existing contractors
- Review existing contracts for AI governance gaps
- Assess your current oversight capabilities

#### Week 3-4: Governance Structure

- Establish AI governance roles and responsibilities
- Develop tier classification criteria
- Draft standard AI governance clauses for contracts
- Coordinate with agency CAIO

### Phase 2: Contractor Oversight (Weeks 5-8)

#### Week 5-6: Evidence Collection

- Request evidence packages from contractors for Tier 1/2 systems
- Validate contractor tier classifications
- Identify gaps in contractor documentation
- Develop remediation requirements for non-compliant contractors

#### Week 7-8: Verification Procedures

- Establish verification activities by tier
- Conduct initial verification for Tier 1 systems
- Develop incident reporting and response procedures

### Phase 3: Operationalization (Weeks 9-12)

#### Week 9-10: Contract Integration

- Include AI governance clauses in new solicitations
- Modify existing contracts to add AI oversight (where feasible)
- Train COs and CORs on AI governance requirements

#### Week 11-12: Audit Readiness

- Compile IG-ready documentation for Tier 1 systems
- Conduct mock IG review
- Remediate gaps identified
- Establish ongoing monitoring and reporting cadence

# Chapter 10: Maturity Progression

| Level | Name | What It Looks Like |
|:---:|---|---|
| 1 | Ad Hoc | No systematic AI inventory or oversight; reactive to problems |
| 2 | Aware | AI inventory exists; contracts may lack governance clauses; limited verification |
| 3 | Managed | AI clauses in contracts; evidence packages required; verification activities conducted |
| 4 | Measured | Systematic oversight; performance metrics tracked; continuous improvement |
| 5 | Optimized | Evidence-based governance; cryptographically verifiable compliance; real-time visibility |

## Level 5: Cryptographically Verifiable Governance

At the highest maturity level, you don't just require evidence—you require verifiable proof. Contractor AI systems produce cryptographic artifacts that answer "how do you know?" with mathematical certainty.

> **The Audit Artifact:** At Level 5, every consequential AI decision produces a cryptographic record containing: immutable decision record, algorithm version, input/output hashes, policy compliance verification, and replay instructions.

Organizations pursuing Level 5 should evaluate infrastructure vendors (including FERZ, which developed the frameworks in this guide) that provide cryptographically verifiable runtime governance that transforms AI oversight from trust-based to evidence-based.

## Appendix A: AI Inventory Template

Use this template to inventory AI systems on your contracts:

| Field | Description |
|---|---|
| Contract Number | Contract/task order reference |
| Contractor | Prime contractor name |
| AI System Name | System identifier |
| Description | What the AI does |
| Governance Track | Decisioning / Communications / Both |
| Rights-Impacting? | Yes/No with rationale |
| Safety-Impacting? | Yes/No with rationale |
| Tier Classification | Tier 1/2/3/4 with rationale |
| Evidence Package Status | Received / Pending / Gap identified |
| Last Verification Date | Date of last government verification |
| Next Review Due | Date of next scheduled review |

## Appendix B: Tier 1 Approval Checklist

Complete before approving deployment of any Tier 1 AI system:

<div style="border: red;">

**TIER 1 APPROVAL CHECKLIST — Complete before deployment authorization**

- ☐ ☐ AI System in contract inventory with tier classification documented
- ☐ ☐ Automatic Tier 1 triggers reviewed and confirmed
- ☐ ☐ Complete evidence package received from contractor
- ☐ ☐ Training data documentation reviewed for representativeness
- ☐ ☐ Validation results reviewed including demographic subgroup analysis
- ☐ ☐ Human oversight procedures verified as meaningful (not checkbox)
- ☐ ☐ Incident history reviewed; no unresolved issues
- ☐ ☐ Monitoring procedures in place; thresholds defined
- ☐ ☐ Incident reporting path confirmed (contractor to COR to CO)
- ☐ ☐ IG-ready documentation compiled
- ☐ ☐ Agency CAIO notified (if required by agency policy)

Approval Signature: _____ Date: _____

</div>

## Appendix C: PWS/SOW Clause Quick Reference

| Clause | When to Include | Key Provisions |
|---|---|---|
| **AI System Definition** | Every contract that may involve AI | Broad definition including algorithmic/statistical systems; defines Governed Unit; notification requirement |
| **AI Inventory and Classification** | Every contract with AI | Inventory requirement; tier classification; government reclassification right |
| **Tier 1 Requirements** | Contracts with Tier 1 AI | Evidence package; CO approval; 48-hour incident notification |
| **AI Suspension Authority** | Tier 1 / safety-impacting AI | Government stop-the-line authority; 24-hour suspension; pending investigation |
| **AI Audit Rights** | Every contract with AI | Government/IG access; 5-day documentation response; subcontractor access |
| **Flow-Down** | Prime contracts with AI | Subcontractor AI compliance; prime responsibility |
| **GenAI Controls** | Contracts with generative AI | Data input controls; human review; NARA-aligned records retention |

For questions on implementation or to discuss cryptographically verifiable governance infrastructure: ferz.ai