AI GOVERNANCE EXECUTIVE GUIDE SERIES • VOLUME 4

AI Governance for Government Contractors

Winning Work, Protecting Relationships, Surviving Audits

A Practical Guide for Delivering Best-Value AI Services to Federal Customers

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

The contractors who win will be the ones who can prove governance, not just promise it.

FOR

Chief Technology Officers • Program Managers • Capture Managers

Proposal Teams • Compliance Officers • AI/ML Technical Leads

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

Chief Technology Officers, Program Managers, Capture Managers, Proposal Teams, Compliance Officers, and AI/ML Technical Leads at federal contractors, defense primes, systems integrators, and government IT service providers.

Core Thesis

> The contractors who win will be the ones who can prove governance, not just promise it.

The Opportunity

Federal buyers are getting smarter about AI governance. They're adding specific clauses to contracts. They're requiring evidence packages. They're learning what questions to ask. The contractors who are ready for this shift will win work; the ones who aren't will scramble and lose.

Five Ways Governance Readiness Wins

Advantage	How It Works
Win More Contracts	When RFPs require AI governance, you already have it. Competitors scramble.
Reduce Proposal Risk	Pre-built evidence packages are reusable. "We have this" beats "we'll build it."
Survive Audits	When IG comes, you have documentation. Primes without it become case studies.
Protect Relationships	No AI incidents the government learns about from FOIA or complaints.
Command Premium Pricing	"Governance-ready on Day 1" justifies higher rates than "we'll figure it out."

What's Coming in Federal Contracts

Government buyers are increasingly including AI-specific requirements:

- **AI System definitions:** Broad definitions that catch "analytics" and embedded AI — not just ML models
- **Governed Unit concept:** Each use case governed independently, not just "the model"
- **Evidence packages:** Training data provenance, validation results, bias testing, incident history
- **Audit rights:** Government and IG access to documentation, personnel, test environments
- **Suspension authority:** Government can stop your AI pending investigation

This guide shows you how to be ready.

 •

Executive Summary

The federal AI governance landscape is shifting. Agencies are implementing OMB M-24-10, designating Chief AI Officers, and—critically—flowing requirements down to contractors. The days of "trust us, our AI works" are ending. The era of "prove it" has begun.

This is not a compliance burden. This is a competitive opportunity.

Most of your competitors are not ready. They don't have evidence packages. They can't produce training data documentation on request. They don't know what a "Governed Unit" is. When the new contract clauses hit, they will scramble, delay, and lose.

You can be ready. This guide shows you how.

The Government Buyer's New Playbook

Federal program managers now have guidance on what to require from contractors. They're being told to:

- Define AI broadly—including statistical and algorithmic systems, not just "machine learning"
- Require notification of all AI systems within 30 days of use
- Demand evidence packages scaled to risk tier
- Reserve the right to reclassify your AI to a higher tier
- Conduct verification activities, not just accept your assertions
- Suspend AI operations pending investigation

This isn't theoretical. These clauses are appearing in solicitations now. Expect them first in new awards and recompetes, then as modifications on incumbents—typically after an incident or IG pressure.

What This Guide Provides

- **Contract clause decoder:** What the new AI clauses mean and how to respond
- **Evidence package templates:** What to pre-build so you're ready on Day 1
- **Tier classification guidance:** How to self-assess honestly and avoid reclassification surprises
- **Subcontractor management:** How to get what you need from your AI vendors
- **Proposal language:** How to make governance readiness a discriminator
- **Audit survival:** How to be the contractor that doesn't become a case study

The Bottom Line

Government buyers are learning to ask: "How do you know your AI is governed?" The contractors who can answer with evidence—not assertions—will win. The ones who can't will explain to their leadership why they lost.

PART I

The New Landscape

Chapter 1: What Government Buyers Now Expect

Federal acquisition of AI is maturing. Program managers, COs, and CORs are getting training on AI oversight. OMB M-24-10 is being implemented. IG offices are adding AI to their audit plans. This chapter explains what's changing and why it matters to your business.

The OMB M-24-10 Effect

OMB Memorandum M-24-10 requires agencies to govern AI—including AI that contractors operate. Key implications for you:

- **Agency AI inventories include your systems:** If you're running AI on a federal contract, it's in (or should be in) the agency's inventory.
- **Rights-impacting and safety-impacting classifications:** If your AI affects citizen rights or safety, heightened requirements apply—to you.
- **Minimum practices flow down:** Agencies must ensure contractor AI meets standards. That means contract requirements.

> **Agency-Specific Requirements:** OMB M-24-10 is the floor, not the ceiling. DoD, DHS, HHS, VA, and other agencies have additional AI directives. Know your customer's specific requirements.

The New Contract Clauses

Government buyers are adding AI-specific clauses to PWS/SOW. Here's what to expect:

AI System Definition

The definition is broad—deliberately. It includes:

- Machine learning, neural networks, NLP, computer vision
- Statistical, algorithmic, or rule-based decision systems that materially influence outcomes
- AI embedded in commercial products
- AI from your subcontractors

Don't try to argue "it's not really AI." If it materially influences outcomes, it's covered.

Governed Unit Concept

The "Governed Unit" is an AI system performing a specific use case in a specific workflow. The same model in two different contexts = two Governed Units, each independently classified and governed.

Why this matters: You can't just validate "the model" and call it done. Each deployment context requires its own governance.

Evidence Package Requirements

For Tier 1 (high-risk) AI, expect requirements to provide:

- Training data documentation (sources, demographics, selection criteria, limitations)
- Validation results including demographic subgroup analysis
- Bias and fairness testing methodology and results

 •

- Human oversight procedures with proof they're meaningful
- Incident history and corrective actions
- Ongoing monitoring procedures and data

Government Verification Rights

The government is no longer just accepting your assertions. New clauses give them:

- Right to audit AI documentation
- Access to personnel for interviews
- Access to test environments for independent validation
- 5-day response requirement for documentation requests
- Authority to suspend AI operations pending investigation

> ✓ **COMPETITIVE ADVANTAGE:** Contractors who have evidence packages ready can respond in 5 days. Competitors who don't will miss deadlines, trigger escalations, and damage relationships.

Chapter 2: The Competitive Landscape

AI governance readiness is becoming a differentiator. This chapter explains how to position yourself against competitors who aren't ready.

Where Most Contractors Are Today

Honest assessment: most federal contractors are not ready for the new AI governance requirements. Common gaps:

- **No AI inventory:** They don't actually know what AI is running on their contracts
- **No training data documentation:** They can't explain where the data came from or its limitations
- **No subgroup testing:** They validated overall performance but not across demographic groups
- **Checkbox human oversight:** Someone clicks "approve" but doesn't actually review
- **No incident history:** Problems happened but weren't documented as AI incidents
- **Subcontractor black boxes:** They're using vendor AI but can't get governance documentation

What "Governance Ready" Looks Like

Capability	Not Ready	Ready
AI inventory	"We'll figure out what we have"	Complete inventory with tier classifications
Training data	"The vendor handles that"	Documented provenance, demographics, limitations
Validation	"It passed our tests"	Subgroup analysis, bias testing, limitations documented
Human oversight	"Someone approves it"	Defined authority, training, time allocation, accountability
Incidents	"We fix problems"	Documented incident history with root cause and remediation
Subcontractors	"They're compliant"	Evidence packages on file, audit rights in subcontracts

Making Governance a Proposal Discriminator

When responding to RFPs with AI governance requirements, don't just say "we will comply." Show you already can:

Proposal Language That Wins

- "Our AI governance framework is already aligned with OMB M-24-10 and NIST AI RMF."
- "We maintain evidence packages for all Tier 1 AI systems, including [specific artifacts]."
- "Our standard subcontracts include AI governance flow-down and audit rights."
- "We can provide the required evidence package within [X] days of contract award."
- "Our AI incident response procedure has been tested and documented."

Proof Points to Include

- Sample (redacted) evidence package from similar engagement
- AI governance organizational chart with named roles
- List of pre-validated AI tools with governance documentation
- Training records showing AI governance competency

✓ **COMPETITIVE ADVANTAGE:** "We already have this" beats "we will develop this" every time. Pre-built governance artifacts are reusable competitive assets.

PART II

Building Your Governance Capability

Chapter 3: Evidence Packages

Evidence packages are the core deliverable of AI governance. This chapter shows you what to build, how to maintain it, and how to make it reusable across contracts.

Tier 1 Evidence Package Contents

For high-risk AI (rights-impacting, safety-impacting, mission-critical), build and maintain:

Artifact	Contents	Update Frequency
System Description	Architecture, intended use, decision authority, limitations, contraindications	On change
Training Data Doc	Sources, demographics, selection criteria, known gaps, provenance chain	On retraining
Validation Report	Performance metrics overall and by subgroup, test methodology, limitations	Annual + on change
Bias/Fairness Testing	Methodology, protected class proxies tested, results, remediation	Annual + on change
Human Oversight SOP	Reviewer roles, authority, training requirements, time allocation, escalation	Annual review
Incident Log	All incidents, root cause, corrective actions, government notifications	Continuous
Monitoring Dashboard	Metrics tracked, thresholds, drift detection, alert procedures	Continuous

Building Evidence Packages Efficiently

Evidence packages shouldn't be one-off efforts. Build infrastructure:

- **Templates:** Standardized templates for each artifact type, pre-populated where possible
- **Automation:** Automated collection of monitoring data, incident logs, validation metrics
- **Version control:** All artifacts versioned with clear change history
- **Central repository:** Single source of truth accessible to program teams and auditors
- **Review calendar:** Scheduled reviews to ensure currency

What Government Reviewers Look For

When evaluating your evidence package, government reviewers (and IG auditors) look for:

- **Completeness:** All required artifacts present, no obvious gaps
- **Currency:** Documents reflect current system state, not outdated versions
- **Specificity:** Concrete details, not generic boilerplate
- **Honesty about limitations:** Documented constraints are more credible than claims of perfection
- **Traceability:** Can trace from requirements to testing to deployment

Red Flags That Trigger Deeper Review

- Generic descriptions that could apply to any AI system
- Validation results that are too good (no limitations documented)

- Human oversight procedures with no time allocation or training requirements
- Empty incident logs ("no incidents" is less credible than "incidents with resolution")
- Subcontractor AI with no governance documentation

✓ **COMPETITIVE ADVANTAGE:** An evidence package that honestly documents limitations is more credible than one that claims perfection. Reviewers know AI has limitations; they want to see you've identified and managed them.

Chapter 4: Tier Classification

Classifying your AI correctly is critical. Under-classify and you'll be reclassified by the government—with delay and credibility damage. Over-classify and you'll burden yourself with unnecessary overhead. Get it right the first time.

The Four Tiers

Tier	Criteria	Examples	What You Must Provide
Tier 1	Rights-impacting, safety-impacting, mission-critical	Eligibility, threat detection, autonomous systems	Full evidence package, CO approval before deployment
Tier 2	Operational impact, federal employee-facing	Caseworker tools, document processing	Validation summary, annual review, monitoring
Tier 3	Internal, no citizen impact	Meeting transcription, internal search	Basic documentation, security controls
Tier 4	Personal productivity, no gov data	General research tools	Acceptable use policy only

Automatic Tier 1 Triggers

These conditions make any AI system Tier 1, regardless of your assessment:

- Outputs substantially factor into decisions affecting civil rights or equal opportunity
- Outputs substantially factor into decisions affecting human safety or critical infrastructure
- Produces citizen-facing determinations (even with "human review")
- Involves classified, CUI, or sensitive PII in decision logic
- Has autonomous or semi-autonomous action capability

Don't try to argue around these. If a trigger applies, classify as Tier 1.

The "Governed Unit" Trap

Remember: governance applies to each Governed Unit (AI + use case + workflow), not just "the model." Common mistakes:

- **Wrong:** "Our NLP model is Tier 3 because it's just text processing."
- **Right:** "Our NLP model processing benefits applications is Tier 1; the same model doing internal search is Tier 3."

The government can reclassify any Governed Unit to a higher tier. If you've under-classified, you'll have to produce Tier 1 documentation on short notice—or face suspension.

> ✓ **COMPETITIVE ADVANTAGE:** Classify honestly. A Tier 1 classification with solid documentation is better than a Tier 3 classification that gets overruled with credibility damage.

Chapter 5: Managing Subcontractors and Vendors

If you're using AI from subcontractors or commercial vendors, you're responsible for their governance. "The vendor handles that" is not an acceptable answer to a government auditor.

The Prime Contractor's Problem

As prime, you face the government. When the CO asks for an evidence package, you must provide it—even if the AI comes from a subcontractor. When the IG audits, they audit you.

Common failure modes:

- **Vendor black box:** Commercial AI vendor won't provide training data documentation
- **Subcontractor resistance:** Sub claims governance artifacts are "proprietary"
- **Missing flow-down:** Your subcontract doesn't include AI governance requirements
- **No audit rights:** You can't actually verify sub's claims

What to Require from Subcontractors

Include in every subcontract involving AI:

Requirement	Tier 1	Tier 2	Tier 3
AI system description and intended use	Required	Required	Required
Training data provenance documentation	Required	Required	N/A
Validation results with subgroup analysis	Required	Summary	N/A
Bias/fairness testing results	Required	Risk-based	N/A
Incident history and remediation	Required	Required	Requested
Audit/inspection cooperation	Required	Required	Required
Government access rights (flow-through)	Required	Required	Required

Negotiating with Resistant Vendors

Some vendors will push back on governance requirements. Responses:

"That's proprietary." → "We need governance documentation, not source code. If you can't provide it, we'll find a vendor who can."

"No one else asks for this." → "Federal contracts now require it. We need vendors who can meet federal requirements."

"We're SOC 2 certified." → "SOC 2 doesn't cover AI governance. We need AI-specific documentation."

"Our AI is too complex to document." → "Then it's too complex to deploy on federal contracts."

Building a Governance-Ready Vendor List

Proactively identify vendors who can meet governance requirements:

- Send AI governance requirements to potential vendors before you need them
- Evaluate governance capability as part of vendor selection
- Maintain a list of "governance-ready" vendors for rapid proposal response
- Include governance requirements in master agreements, not just task orders

✓ **COMPETITIVE ADVANTAGE:** A pre-qualified list of governance-ready vendors is a competitive asset. When RFPs require AI governance, you can respond immediately while competitors negotiate with vendors.

PART III

Operations and Compliance

Chapter 6: Day-to-Day Governance Operations

Governance isn't a one-time deliverable—it's ongoing operations. This chapter covers the operational rhythm that keeps you compliant and audit-ready.

The Governance Calendar

Frequency	Activity	Owner
Continuous	Monitoring data collection, incident logging	Technical team
Monthly	Monitoring review, threshold check, drift assessment	AI governance lead
Quarterly	Evidence package currency review, subcontractor check-in	Program manager
Annual	Full revalidation (Tier 1), bias retesting, policy review	AI governance lead
On change	Impact assessment, re-tiering evaluation, documentation update	Technical team + governance

Incident Management

AI incidents will happen. How you handle them determines whether they become audit findings.

What Counts as an Incident

- AI produces incorrect output affecting citizen or mission outcome
- Performance degrades below validated thresholds
- Bias or disparate impact is identified
- Human oversight is bypassed (intentionally or accidentally)
- Data quality issue affects AI operation
- Security event involving AI system

Incident Response Requirements

- **48-hour notification:** Government contracts typically require notification within 48 hours for Tier 1 AI incidents. Know your contract's specific requirement.
- **Root cause analysis:** Determine why it happened, not just what happened
- **Corrective action:** Document what you're doing to prevent recurrence
- **Evidence preservation:** Preserve logs, data, and system state for potential audit

The Incident Log

Maintain a continuous incident log containing:

- Date/time of incident and detection
- Description of what happened
- Impact assessment
- Root cause (when determined)
- Corrective actions taken
- Government notification (if required) with date and recipient
- Resolution and closure

✓ **COMPETITIVE ADVANTAGE:** A well-documented incident history shows mature governance. An empty incident log raises suspicion that you're not detecting problems—not that you don't have them.

Chapter 7: Surviving Audits

IG audits of AI are increasing. This chapter prepares you to survive—and even benefit from—audit scrutiny.

What Auditors Ask For

Based on emerging IG audit practices, expect requests for:

Inventory and Classification

- Complete list of AI systems on this contract
- Tier classification for each with rationale
- Evidence of government notification within required timeframes

Evidence Packages

- Training data documentation
- Validation results
- Bias testing methodology and results
- Human oversight procedures

Operational Records

- Monitoring data for past 12 months
- Incident log with all entries
- Government notifications made
- Corrective actions taken and evidence of effectiveness

Subcontractor Oversight

- List of subcontractors providing AI
- Evidence packages from each
- Your verification activities

The 5-Day Response

New contract clauses require documentation within 5 business days of government request. If you can't respond in time:

- Credibility damage with program office
- Potential escalation to CO
- Audit finding for "inadequate documentation"
- Contract performance issue

If you've built your evidence packages and maintained them, 5 days is easy. If you haven't, it's impossible.

Common Audit Findings to Avoid

Finding	How to Avoid It
Incomplete AI inventory	Know what AI is running. Include embedded AI and subcontractor AI.
Missing evidence packages	Build and maintain packages before you need them.
Inadequate training data documentation	Document provenance, demographics, and limitations.
No subgroup validation	Test performance across demographic groups, not just overall.
Checkbox human oversight	Document authority, training, time allocation—prove it's meaningful.
Unreported incidents	Log everything. Report per contract requirements.
Subcontractor gaps	Get evidence packages from subs. Don't accept "proprietary."

✓ **COMPETITIVE ADVANTAGE:** The best audit outcome is "no findings." The second best is "findings already remediated." Build governance so you get one of these.

PART IV

Building Your Capability

Chapter 8: Organizational Readiness

AI governance requires organizational capability, not just documentation. This chapter covers the people, processes, and authority you need.

Key Roles

Role	Responsibilities	Required Competencies
AI Governance Lead	Policy, standards, evidence package oversight, audit coordination	AI basics + federal compliance + program management
Technical AI Lead	Validation, monitoring, incident investigation, documentation accuracy	ML/AI technical depth + validation methodologies
Program AI POC	Contract-specific governance, government liaison, evidence delivery	Contract knowledge + AI awareness + communication
Subcontract Manager	Vendor/sub AI requirements, evidence collection, flow-down	Procurement + AI governance requirements

Authority Requirements

Governance fails when the function lacks authority. Ensure:

- **Tier classification authority:** AI governance lead can classify and escalate, not just recommend
- **Deployment gates:** No Tier 1 AI deploys without governance sign-off
- **Budget:** Validation, testing, and documentation have dedicated budget—not borrowed from delivery
- **Escalation path:** Clear path to stop deployment if governance is inadequate

Competency Development

Your people need to understand AI governance—not just check boxes.

- **AI basics:** What is AI, how does it work, what are common failure modes
- **Federal requirements:** OMB M-24-10, agency-specific requirements, contract clauses
- **Validation methods:** How to evaluate bias testing, subgroup analysis, monitoring data
- **Evidence package contents:** What belongs in each artifact, what reviewers look for

Process Infrastructure

- Templates for all evidence package artifacts
- Checklists for tier classification
- Workflow for government notifications
- Calendar for periodic reviews
- Repository for evidence packages with access controls
- Incident response playbook

Chapter 9: Implementation Roadmap

If you're starting from scratch, here's how to build governance capability in 90 days.

Phase 1: Foundation (Weeks 1-4)

Week 1-2: Inventory and Assessment

- Identify all AI on current federal contracts (including embedded and subcontractor AI)
- Assess current state of documentation for each
- Identify gaps against Tier 1 evidence requirements
- Review current subcontracts for AI governance provisions

Week 3-4: Structure and Standards

- Assign AI governance roles
- Establish tier classification criteria
- Create evidence package templates
- Draft standard subcontract AI provisions

Phase 2: Build (Weeks 5-8)

Week 5-6: Evidence Packages

- Prioritize Tier 1 and Tier 2 systems
- Build evidence packages for highest-risk systems first
- Request evidence from subcontractors
- Identify vendor gaps and negotiate solutions

Week 7-8: Operations

- Implement monitoring for Tier 1 systems
- Establish incident logging
- Create governance calendar
- Test 5-day response capability

Phase 3: Operationalize (Weeks 9-12)

Week 9-10: Integration

- Integrate governance into proposal process
- Add AI governance to subcontract templates
- Train program teams on governance requirements
- Brief capture teams on competitive positioning

Week 11-12: Validation

- Conduct mock audit
- Remediate gaps identified
- Document lessons learned
- Establish continuous improvement process

> ✓ **COMPETITIVE ADVANTAGE:** 90 days gets you from zero to governance-ready. Competitors who wait will need 90 days after the RFP drops—and won't have it.

Chapter 10: Maturity Progression

Governance capability develops over time. Here's the progression from basic compliance to competitive advantage.

Level	Name	What It Looks Like	Business Value
1	**Reactive**	Build documentation when asked	Can respond (slowly) to requirements
2	**Structured**	Standard templates, assigned roles	Faster response, consistent quality
3	**Managed**	Pre-built packages, proactive monitoring	Proposal discriminator, audit-ready
4	**Optimized**	Automated collection, predictive risk ID	Premium positioning, minimal overhead
5	**Verifiable**	Cryptographic proof of governance	"How do you know?" answered definitively

Level 5: Cryptographically Verifiable Governance

At the highest maturity, you don't just assert governance—you prove it. Every consequential AI decision produces a cryptographic artifact that independently verifies compliance.

This transforms the audit conversation from "show me your documentation" to "here's mathematical proof." It also transforms the competitive conversation from "trust us" to "verify it yourself."

Organizations pursuing Level 5 should evaluate infrastructure vendors (including FERZ, which developed the frameworks in this guide) that provide cryptographically verifiable runtime governance.

> **The Authorization Boundary:** Governance is the point where outputs become decisions, and where evidence—not explanations—must exist. Level 5 makes that evidence irrefutable.

 •

Appendix A: Evidence Package Checklist

Use this checklist to verify evidence package completeness before government submission:

TIER 1 EVIDENCE PACKAGE — Complete before deployment or submission

- ☐ ☐ AI System description with intended use and limitations
- ☐ ☐ Governed Unit definition (use case + workflow + decision authority)
- ☐ ☐ Tier classification with rationale and trigger assessment
- ☐ ☐ Training data documentation (sources, demographics, selection, limitations)
- ☐ ☐ Validation report with performance metrics overall and by subgroup
- ☐ ☐ Bias/fairness testing methodology and results
- ☐ ☐ Human oversight SOP (roles, authority, training, time allocation)
- ☐ ☐ Incident log (complete history, not just "no incidents")
- ☐ ☐ Monitoring procedures with metrics, thresholds, and alert process
- ☐ ☐ Subcontractor evidence packages (if applicable)
- ☐ ☐ All documents current (updated within required timeframe)

Appendix B: Contract Clause Response Guide

When you see these clauses in RFPs or contracts, here's what to prepare:

Clause Type	What It Requires	What You Need Ready
AI System Definition	Broad scope including analytics/algorithms; notification of use	Complete AI inventory; notification process
Governed Unit	Each use case governed independently	Per-use-case documentation, not just "the model"
Tier Classification	Risk-based classification; government can reclassify	Honest self-assessment; Tier 1 readiness for borderline cases
Evidence Package	Training data, validation, bias testing, oversight, incidents	Pre-built packages; 5-day response capability
Audit Rights	Government access to docs, personnel, test environments	Organized repository; identified SMEs; test environment access
Suspension Authority	Government can stop AI pending investigation	Incident response plan; rollback capability; rapid remediation
Flow-Down	Must flow requirements to subcontractors	Standard sub provisions; vendor evidence packages on file

 •

Appendix C: Proposal Differentiator Language

Sample language to demonstrate governance readiness in proposals:

AI Governance Framework

> "[Company] maintains an enterprise AI governance framework aligned with OMB M-24-10 and NIST AI RMF. Our framework includes tiered classification of AI systems, standardized evidence packages, continuous monitoring, and incident response procedures. For this requirement, we have pre-classified [system] as Tier [X] and can provide the complete evidence package within [X] days of award."

Evidence Package Readiness

> "Our standard AI evidence package includes training data provenance documentation, validation results with demographic subgroup analysis, bias testing methodology and results, human oversight procedures, incident history, and monitoring procedures. [Attached/available upon request] is a sample evidence package from a comparable [unclassified] engagement demonstrating our documentation standards."

Subcontractor Management

> "Our subcontract template includes AI governance flow-down requirements and audit rights. We maintain evidence packages from all AI subcontractors and can provide government access to subcontractor documentation as required. Our proposed [subcontractor] has confirmed ability to meet Tier [X] evidence requirements."

Audit Readiness

> "[Company] maintains IG-ready documentation for all AI systems on federal contracts. Our AI governance repository enables response to documentation requests within the 5-day contract requirement. We have successfully supported [X] AI-related audits without material findings."

 •

Appendix D: Proposal Pack Insert (Copy/Paste Ready)

Insert this section into proposals responding to AI governance requirements. Customize bracketed items.

AI GOVERNANCE APPROACH

[Company] delivers AI capabilities with governance infrastructure that meets federal requirements from Day 1. Our approach is built on OMB M-24-10 alignment, NIST AI RMF principles, and evidence-based verification—not assertions. We classify each AI use case as a Governed Unit with independent documentation, maintain pre-built evidence packages for rapid deployment, and operate continuous monitoring with defined escalation paths. For this requirement, we have assessed [system/capability] as Tier [1/2/3] based on [rationale] and can deliver the complete evidence package within [30] days of award. Our governance infrastructure has supported [X] federal AI deployments without material audit findings.

Requirement-to-Artifact Mapping

Government Requirement	Our Artifact	Delivery
AI System inventory and notification	Governed Unit Registry	Day 1
Tier classification with rationale	Tier Classification Memo	Day 1
Training data documentation	Training Data Provenance Report	Day 30
Validation with subgroup analysis	Validation & Bias Testing Report	Day 30
Human oversight procedures	Human Oversight SOP	Day 30
Monitoring and drift detection	Monitoring & Drift Plan	Day 30
Incident response	Incident Response Playbook	Day 1
Subcontractor governance	Subcontractor Flow-Down Addendum	Day 1

AI Governance Deliverables

1. Tier 1 Evidence Package v[X] — Complete governance documentation per Section H.XX requirements
2. Governed Unit Registry — Inventory of all AI systems with tier classification and rationale
3. Monitoring & Drift Plan — Metrics, thresholds, alert procedures, and review cadence
4. Incident Response Playbook — Detection, escalation, notification, and remediation procedures
5. Subcontractor Flow-Down Addendum — Standard AI governance provisions for all AI subcontracts
6. Quarterly Governance Report — Status, metrics, incidents, and remediation summary
7. Annual Revalidation Report — Full validation refresh for Tier 1 systems

 •

Appendix E: Evidence Package Table of Contents

Standardize your evidence packages with this structure. Government reviewers evaluate completeness, currency, specificity, and traceability.

TIER 1 EVIDENCE PACKAGE — Standard Table of Contents

Section 1: Executive Summary

1.1 System identification and Governed Unit definition
1.2 Tier classification with rationale and trigger assessment
1.3 Package version and currency statement (last updated: [date])

Section 2: System Description

2.1 Architecture and technical approach
2.2 Intended use and decision authority boundaries
2.3 Known limitations and contraindications

Section 3: Training Data Documentation

3.1 Data sources and provenance chain
3.2 Demographic composition and representativeness analysis
3.3 Selection criteria and preprocessing
3.4 Known gaps and limitations

Section 4: Validation Report

4.1 Validation methodology and test dataset description
4.2 Performance metrics (overall)
4.3 Performance metrics (by demographic subgroup)
4.4 Bias and fairness testing methodology and results
4.5 Identified limitations and operating constraints

Section 5: Human Oversight

5.1 Reviewer roles, authority, and accountability
5.2 Training requirements and records
5.3 Time allocation and workload analysis
5.4 Escalation procedures

Section 6: Monitoring and Operations

6.1 Metrics tracked and thresholds
6.2 Drift detection approach
6.3 Alert and escalation procedures
6.4 Review cadence

Section 7: Incident History

7.1 Incident log (complete)
7.2 Root cause analyses
7.3 Corrective actions and effectiveness verification

Section 8: Subcontractor Documentation (if applicable)

8.1 Subcontractor AI inventory
8.2 Evidence packages from each subcontractor
8.3 Flow-down verification

Appendices

A. Approval signatures and dates
B. Version history
C. Supporting technical documentation (references)

 •

Appendix F: Credible Delivery Timeline

Use this timeline to make realistic commitments. Overpromising destroys credibility; underpromising loses contracts. This is what governance-ready contractors can actually deliver.

Day 1 Deliverables (Contract Award)

What you should have ready before award, delivered immediately:

Deliverable	Contents	Pre-Condition
Governed Unit Registry	Complete inventory of AI with tier classifications	Pre-built from proposal analysis
Tier Classification Memo	Rationale for each classification, trigger assessment	Completed during proposal
Incident Response Playbook	Detection, escalation, notification procedures	Standard template customized
Subcontractor Flow-Down Addendum	Standard AI governance provisions	Pre-negotiated with subs
Governance POC Designation	Named individuals with contact info	Staffing plan confirmed

Day 30 Deliverables

What requires contract-specific work but can be completed quickly:

Deliverable	Contents	Effort Required
Training Data Documentation	Provenance, demographics, limitations	Compile from existing records + gap analysis
Validation Report (Initial)	Performance metrics, subgroup analysis	Run validation suite on deployed config
Human Oversight SOP	Roles, authority, training, time allocation	Customize standard template to contract
Monitoring & Drift Plan	Metrics, thresholds, alerting	Configure monitoring for specific deployment

Day 90 Deliverables

What requires operational data and extended effort:

Deliverable	Contents	Dependency
Complete Evidence Package	All sections populated, reviewed, approved	Day 30 deliverables + operational experience
Bias/Fairness Deep Dive	Extended testing across all relevant subgroups	Sufficient operational data
First Quarterly Report	Metrics, incidents, governance status	90 days of monitoring data
Subcontractor Evidence Packages	Complete packages from all AI subs	Sub delivery + your verification

> **Proposal Guidance:** Commit to Day 1 and Day 30 deliverables in your proposal. Reference Day 90 as the complete evidence package milestone. Never promise Day 1 delivery of items that genuinely require operational data.

Appendix G: What NOT to Claim (Credibility Protection)

These claims destroy credibility with sophisticated government reviewers. Avoid them.

NEVER CLAIM:

✗ **"100% accuracy" or "no false positives"**

→ All AI has error rates. Claiming perfection signals you don't understand AI or you're hiding limitations.

✗ **"The vendor handles governance"**

→ You face the government, not the vendor. This signals you can't produce evidence when asked.

✗ **"It's not AI, it's analytics/statistics/rules"**

→ Contract definitions are broad. This signals you're trying to evade governance requirements.

✗ **"No incidents to report"**

→ Empty incident logs suggest you're not detecting problems, not that you don't have them. Document issues with resolutions.

✗ **"Fully explainable AI" (without qualification)**

→ Explainability is a spectrum. Specify what level you actually provide and for which decisions.

✗ **"Human in the loop" (without specifics)**

→ Checkbox approvals don't count. Specify authority, training, time allocation, and accountability.

✗ **"Proprietary methodology" (as reason for no documentation)**

→ Government has audit rights. "Proprietary" isn't a shield against evidence requirements.

✗ **"Tier 3" for anything citizen-facing or rights-affecting**

→ Government can reclassify. Under-tiering will be caught and damages credibility.

Instead, demonstrate mature governance by honestly documenting limitations, quantifying error rates, and showing how you manage the risks you've identified. Credibility comes from realism, not perfection.

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

