PROGRAM SUPPORT · AI GOVERNANCE

De-risking Federal AI Acquisition

How program offices can buy and govern AI they can defend — turning the NIST AI Risk Management Framework into contract language, test criteria, and off-ramps.

 Intelligence. Integrity. Impact.

Program Support · AI Governance

Buying AI is not buying software. Software does what it was written to do; AI does what it learned to do, and what it learned can drift, degrade, and surprise you after the contract is signed. Program offices that acquire AI the way they acquire a database — pay, accept, deploy — inherit a system nobody can fully explain and no one agreed to govern. This paper is about buying AI you can actually defend.

AI is a different kind of buy

4

Functions in the NIST AI Risk Management Framework — Govern, Map, Measure, Manage.

NIST AI RMF 1.0

CAIO

The Chief AI Officer each agency must now designate to govern AI use.

OMB M-25-21

High-impact

The tier of AI that draws the most oversight — classify the use case right, first.

OMB M-25-21

Why AI acquisition is different

Three properties make AI unlike the software a program office is used to buying. It is **data-dependent** — its behavior is a product of training data the government may not own or even see. It **drifts** — performance that passed acceptance can decay as the world changes underneath it. And it is **opaque** — "it works in the demo" is not evidence that it will work on the mission's data, at the mission's edge cases, under an adversary's pressure. Ordinary acquisition assumes none of these. AI acquisition has to plan for all three.

From framework to contract

The good news is that a framework already exists, and it maps cleanly onto the acquisition instruments a program office already uses. The NIST AI Risk Management Framework's four functions become four sets of contract obligations (Figure 1) — governance is not an abstract aspiration, it is language in the statement of work and criteria in the acceptance plan.

NIST AI RMF function	What it means at acquisition	Contract lever
Govern	Stand up oversight and accountability	Require an AI governance plan; name a responsible official
Map	Define the intended use and its risks	Use-case and risk statement in the SOW; risk-tier classification
Measure	Test, evaluate, and red-team before you rely on it	Independent T&E; performance thresholds as acceptance criteria
Manage	Monitor, respond, and be able to walk away	Monitoring CDRLs; drift triggers; transition and termination rights

Figure 1. The NIST AI Risk Management Framework, translated into acquisition. Each function becomes a concrete contract lever — governance you can enforce, not governance you merely hope for. (Framework: NIST AI RMF 1.0.)

The acquisition lifecycle

Governance is not a one-time gate at award; it is a loop that continues for as long as the system is in use. The use case is defined and risk-tiered, the system is tested and authorized, it is deployed and then monitored — and a drift or an incident routes back to re-evaluation, not to a shrug (Figure 2).

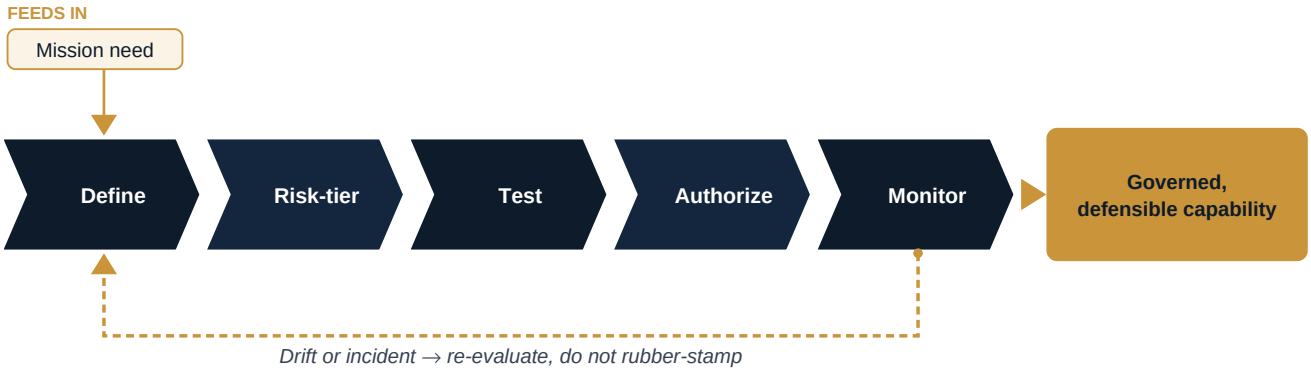

Figure 2. AI acquisition as a governed lifecycle. Testing and authorization are not the finish line; monitoring feeds back into re-evaluation whenever the system drifts or an incident occurs. Buying AI is signing up to keep watching it.

The levers that actually matter

A handful of contract terms do most of the de-risking. Get these right and the rest is detail:

- **Data rights and provenance.** Know what the model was trained on, what rights the government has, and demand a bill of materials for models and dependencies.
- **Independent test and evaluation.** Acceptance rests on results from someone other than the vendor, on the mission's data and edge cases — not the vendor's demo.

- **Monitoring and drift triggers.** Define, in the contract, how performance is watched and what threshold forces a re-evaluation.
- **Off-ramps.** Transition and termination rights, and portable data and interfaces, so a system that stops earning its keep can be replaced without a hostage negotiation.

Red flags in an AI proposal

A few patterns in a vendor proposal reliably predict trouble, and a program office should treat them as hard questions to resolve, not automatic disqualifiers. A refusal to disclose what a model was trained on, or to name its dependencies. Accuracy claims with no reference to the mission's own data or edge cases. A demo that cannot be reproduced on the government's inputs. No answer for what happens when performance drifts. And architectures that make the government's data hard to extract or the model impossible to replace. None of these is necessarily fatal. All of them should be resolved in writing before award, not discovered after it — because after award, the leverage to fix them is gone.

Do not trade one lock-in for another

The fastest way to lose leverage is to build a mission-critical dependency on a model you cannot inspect, move, or replace. Favor arrangements that keep the government's data portable and its options open. An AI capability that cannot be swapped out is not an asset; it is a future emergency with a renewal date.

Buy AI you can defend

The program offices that come out of the AI wave in good shape will not be the ones that bought the flashiest model. They will be the ones that bought AI they could govern — with the intended use written down, the testing independent, the monitoring live, and the exit clear. The framework already exists. The work is the discipline to put it in the contract before the ink is dry, not after the first surprise.

References

1. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, January 2023.
2. National Institute of Standards and Technology, *AI RMF Generative AI Profile*, NIST AI 600-1, 2024.
3. Office of Management and Budget, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, OMB M-25-21, April 2025 (issued under Executive Order 14179).
4. U.S. Government Accountability Office, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, GAO-21-519SP, 2021.
5. Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) — data-rights and acceptance provisions.