Presidential Memorandum

National Security Memo/NSPM-11

June 5, 2026

Overview

President Trump signed NSPM-11, *Artificial Intelligence in the National Security Enterprise*, on June 5, 2026. The memorandum directs the national security enterprise, the Department of War, the Intelligence Community, and agencies serving a national security role, to responsibly accelerate AI adoption while maintaining rigorous oversight and a resilient, secure supply chain. It **rescinds and replaces NSM-25**, the prior administration's AI national security framework.

The memo is built on **four pillars** that define how the national security enterprise must adopt and govern AI:

Pillars	Focus & Key Provisions
Adoption	Accelerate AI adoption by identifying mission areas where AI enhances operational effectiveness and removing barriers to rapid deployment; maintain deep industry partnerships to make frontier models broadly available to national security professionals.
Adaption	Favor commercial and open-source AI from diverse suppliers, large and small, optimized for intended use; build or customize internally only where commercial solutions are not appropriate for security or mission reasons.
Assurance	Ensure AI is reliable, robust, steerable, and controllable; guarantee (via contract or other means) that no vendor or adversary can disable, degrade, or modify a fielded system without Federal knowledge and approval; rigorous TEVV throughout.
Accountability	Prohibit AI used to censor speech, embed ideological bias, or conduct unlawful surveillance; preserve civil liberties and privacy; commanders, directors, and agency heads remain responsible at every level of command.

Key Deadlines & Focus Provisions for Government

The following deadlines apply to **Federal national security agencies**. They set the timeline by which the government must issue guidance and stand up the capabilities below.

Pillars	Focus & Key Provisions
Within 30 Days	All waiver exceptions to the contract-termination directive must be reported in writing to the APST and APNSA.
Within 90 Days	Update DoD Directive 3000.09 (Autonomy in Weapon Systems); issue AI governance policy for National Security Systems (aligned with OMB M-25-21); develop a roadmap for advanced computing access and an AI test range; issue a classified annex.
Within 120 Days	Update procurement for rapid multi-vendor AI onboarding; build private-sector security partnerships (anti-distillation, joint red teams, data-center security) via the AI Security Center; launch joint AI data/model exchanges; stand up an AI National Security Strategic Reserve; develop an AI for National Security curriculum; issue joint AI risk-management and TEVV methodologies.

What Does This Mean for Government?

Agencies are directed to move fast and lean heavily on commercial capability:

- Procure the most advanced frontier models from multiple vendors, closing the gap between public and national-security capabilities, and avoiding single-vendor dependencies.
- Build assurance in from the start: testing, evaluation, verification, and validation (TEVV), plus contractual guarantees that no vendor or adversary can disable/alter a fielded AI system without Federal approval.
- Terminate contracts with companies showing a repeated pattern of conduct inconsistent with the memo's policy (including subcontractors), with a waiver process capped at one year for mission-critical needs.
- Stand up secure compute, classified AI enclaves, an AI test range, and joint data/model exchanges across the enterprise.

Industry Implications

This is a strong national-security AI demand signal, it rewards vendors that can prove security, controllability, and resilience. The memo deliberately favors diverse suppliers (large and small, commercial and open-source) and discourages lock-in, opening doors beyond incumbents.

Where to focus:

- **Named owners first:** Prioritize the Department of War, the Intelligence Community, NSA (and its AI Security Center), DoE (Genesis Mission), DNI, OPM, DHS, and OMB.
- **Prove assurance & controllability:** TEVV, red-teaming, model security, and guardrails are now procurement prerequisites.
- **Design against lock-in:** Open architectures, multi-cloud, and the ability to operate across classified enclaves align directly with the Adaptation pillar.