carahsoft.
TECHNOLOGY BY POLICY

Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting American Producers

November 21, 2025

Overview

Memorandum M-26-02, issued under the authority of the American Security Drones Act, provides comprehensive guidance for federal agencies on the secure use and acquisition of unmanned aircraft systems (UAS). The memo requires agencies to treat UAS as both aircraft and information systems, applying federal cybersecurity and privacy standards throughout their lifecycle. The policy mandates risk-based assessments, encryption of data, secure firmware updates, and multifactor authentication to safeguard sensitive information.

Additionally, it incorporates these security requirements directly into federal procurement workflows and the administration of grant funding, ensuring that agencies and recipients are held to consistent and enforceable standards. By embedding these controls into acquisition processes, the memo helps guarantee that vendors, contractors, and grant-funded entities adhere to robust cybersecurity and supply chain safeguards before participating in federal programs

Key Requirements and Timelines:

- **Implementation Deadline:** By May 20, 2026, agencies must integrate the policy into their procurement and funding process
- **Across Lifecycle:** Agencies must apply security safeguards during acquisition, operation, post-mission and data disposal

What This Means for Vendors

For drone vendors, this memorandum signals both a significant growth opportunity and a heightened compliance challenge, requiring robust security measures and transparent supply chains to remain competitive in the federal market.

- **Stricter Compliance Requirements:** Vendors must ensure their UAS meet federal cyber security and privacy standards, including:
  - Encryption of data at rest and in transit using validated cryptography
  - Secure firmware/software update mechanism from trusted sources
  - Multi-factor authentication for ground control systems
  - Ability to remotely wipe off lock devices and restrict unnecessary data flows
- **Lifecycle Security Integration:** Vendors need to design and document security measures across the entire UAS lifecycle
- **Supply Chain Transparency:** Vendors will be expected to demonstrate secure sourcing of components and compliance with federal acquisition security requirements
- **Preference for U.S Manufactures:** The memo encourages agencies to prioritize domestic UAS producers when security need align, creating opportunities for U.S.-based vendors to gain market share
- **Impact on Grants and Funding:** Vendors selling to non-federal entities using federal grants must also comply with these security standards, as agencies will require recipients to follow the same rules
- **Document & Certification:** Vendors will likely need to provide detailed security documentation, risk, assessments, and possibly third-party certification to prove compliance