EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 21, 2025

M-26-02

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers

Overview

Commercial unmanned aircraft systems (UAS) technology has evolved rapidly and enabled a proliferation of critical use cases across the Federal Government. Examples of civilian uses include enhancing situational awareness of Federal law enforcement, monitoring forest fires, supporting agriculture research activities, and supporting search and rescue operations.

Use of insecure, foreign-manufactured UAS could potentially expose critical U.S. information to data breaches of connected systems, hidden capture of UAS camera feeds, and uncontrollable UAS flight behavior. The U.S. Government and industry rely on American suppliers to produce innovative and secure solutions, and Federal funds should be used to strengthen the domestic manufacturing base for such technologies.

In addition to cybersecurity threats, reliance on foreign-made drones poses broader strategic and economic risks. Depending on foreign-manufactured systems for critical Federal functions could undermine the U.S. drone industry and reduce U.S. technological sovereignty. This dependency also leaves the Federal Government exposed to supply chain disruptions or embedded surveillance capabilities that are difficult to detect. Ensuring the integrity and security of Federal operations requires minimizing reliance on adversarial technology, investing in secure alternatives, and supporting American or allied drone manufacturers aligned with U.S. interests.

Background

The American Security Drone Act ("the Act")[1] instructs the Director of the Office of Management and Budget (OMB) to establish government-wide policy for the procurement of

[1] American Security Drone Act (ASDA), Pub. L. No. 118-31, §§ 1821-32 (41 U.S.C. § 3901 note) (2023).

unmanned aircraft systems (UAS),[2] in coordination with the Secretary of Homeland Security, the Secretary of Transportation, and the Attorney General, and in consultation with the Director of the National Institute of Standards and Technology (NIST).[3] The required policy must include various specifications to help mitigate the risks associated with processing, storing, and transmitting Federal information in a UAS.

This memorandum fulfills those requirements by providing a framework, set forth in Appendices A and B, for agencies[4] to establish a process to address information security risks present when procuring UAS. Pursuant to the Act, the actions outlined in this memorandum concern the procurement of a UAS—

(1) for non-Department of Defense and non-intelligence community operations; and

(2) through grants and cooperative agreements entered into with non-Federal entities.[5]

Accordingly, this memorandum applies to the procurement by Federal agencies of UAS for use in operations other than those of the Department of Defense or the intelligence community, [6] and to Federal agencies' issuance of grants and cooperative agreements providing funds for the procurement of UAS to process, store, or transmit Federal information.[7]

Agency Actions

During use of a UAS, after use of a UAS, and otherwise throughout the information life cycle,[8] agencies that operate or fund the procurement of UAS must apply appropriate safeguards for the protection of Federal information, including privacy data[9] and other controlled unclassified information, that is generated by or otherwise accessible to the UAS, consistent with relevant law and policy. The protections applied to Federal information must be commensurate with the risk associated with unauthorized access, use, disclosure, disruption, modification, or destruction of the data.

Agencies must ensure that their UAS access control policies and implementation of technical controls (e.g., methods of login for the ground control station) conform to applicable requirements in OMB Circular No. A-130, *Managing Information as a Strategic Resource*.

---

[2] As defined in 49 U.S.C. § 44801.
[3] Pub. L. No. 118-31, § 1829.
[4] As defined in 44 U.S. Code § 3502.
[5] Pub. L. No. 118-31, § 1829.
[6] "Intelligence community" has the meaning given in 50 U.S.C. § 3003.
[7] "Federal information" is "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form." OMB Circular No. A-130, *Managing Information as a Strategic Resource*, at 29.
[8] As defined in OMB Circular A-130.
[9] As required by Pub. L. No. 118-31, § 1829(b)(3), this guidance addresses protection of "privacy data and other controlled unclassified information." For purposes of this memorandum, *privacy data* refers to personally identifiable information, as defined in OMB Circular A-130. For example, that may include location information, audio, video, or images that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Policy Assistance

All questions or inquiries concerning this memorandum should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.

APPENDIX

Appendix A: Requirements for UAS Procurement by Agencies or Through Grants or Cooperative Agreements

1. UAS PROCUREMENT BY AGENCIES

No later than 180 days following the issuance of this memorandum, agencies must ensure that any procurement of UAS appropriately recognizes such systems as both aircraft and information technology (IT) systems and integrates the information security[10] risk procedures identified in Appendix B of this memorandum, regardless of where the UAS was manufactured or assembled.[11]

The procedures in Appendix B of this memorandum are relevant, and should be applied, to all phases of the acquisition of a UAS as follows:

- In the market research phase, agencies shall collect information about how the capabilities of various products align with Appendix B, section 2 of this memorandum.

- During acquisition planning and solicitation development, agencies shall ensure that their requirements are described with sufficient detail to enable vendors to provide offers that are responsive to agency information security requirements, based on the impact assessment conducted per Appendix B, section 1 of this memorandum. Additionally, during acquisition and solicitation development, each agency should consider whether it is necessary to award the contract to a particular domestic source or sources in order to create or maintain the required domestic capability for production of UAS. If awarding to a particular domestic source or sources is necessary on that ground, the agency may consider using noncompetitive acquisition procedures, consistent with applicable legal requirements, including the FAR § 6.302-3 and the Competition in Contracting Act.

- When awarding contracts, agencies should, where appropriate, evaluate offerors on criteria relevant to achieving the outcomes identified in Appendix B, section 2 of this memorandum.

- Following product delivery, or during performance of service contracts involving operation of UAS, agencies shall ensure that they have systems in place to effectively implement the relevant technical measures to mitigate security risks.

The requirements above are supplemental to existing procurement laws and regulations, and do not obviate the need for agencies to comply with all other legal requirements that may be applicable to an acquisition of UAS, including FAR subpart 40.2 (prohibiting the procurement and operation of UAS manufactured or assembled by certain foreign entities).

---

[10] As defined in 44 U.S.C. § 3542.
[11] ASDA, § 1829(d)(2).

2. UAS PROCUREMENT THROUGH GRANTS AND COOPERATIVE AGREEMENTS

No later than 180 days following the issuance of this memorandum, agencies issuing grants and cooperative agreements that provide funds to non-Federal entities for the procurement of UAS to process, store, or transmit Federal information shall do the following:

- Include the appropriate information security requirements from Appendix B of this memorandum in Notices of Funding Opportunity (NOFOs) for awards potentially involving the procurement of UAS to process, store, or transmit Federal information; and require non-Federal entities to be responsive to these requirements in any application submitted for grants or cooperative agreements in response to the NOFO. NOFOs shall include requirements for non-Federal entities to describe how they will develop a risk-based approach to applying these requirements to procurement solicitations to potential vendors under the resulting award.

- Conduct risk assessments and evaluate proposals with the appropriate consideration of the non-Federal entity's response to the requirements included in the NOFO related to procuring UAS under the Federal award.

- Include the specific information security requirements from the NOFO in the terms and conditions of grants and cooperative agreements to ensure that the non-Federal entity will incorporate these requirements in procurement solicitations of UAS under the Federal award.

- Monitor the relevant Federal awards to ensure that non-Federal entities are adhering to the information security requirements in the terms and conditions of the award.

See Appendix D of this memorandum regarding additional restrictions that become effective on December 22, 2025.

Appendix B: Section 1829 Guidance on Necessary Security Capabilities of a UAS

1. IMPACT ASSESSMENT

Prior to procuring a UAS through a contract, issuing a grant, or cooperative agreement that funds the procurement of a UAS to process, store, or transmit Federal information, agency personnel responsible for managing information security risk and any agency personnel responsible for operating or overseeing the operation of the UAS must jointly complete an impact assessment utilizing Federal Information Processing Standard (FIPS) 199,[12] or any successor publications. Additionally, those personnel should coordinate with agency personnel responsible for analyzing privacy risks to ensure consistency between the impact assessment required by this guidance and any privacy impact assessment.[13]

In conducting the impact assessment required by this guidance, agencies should identify and document the types of information that may be stored in, processed by, or transferred to or from the UAS. At a minimum, this would include UAS positional data and any audio or video data supported by the UAS.

Agencies should determine for each information type whether a loss of confidentiality, integrity, or availability could be expected to result in a low, moderate, or high potential impact on agency operations, agency assets, or individuals. Making that determination will enable the agency to identify the appropriate security categories and overall system impact level for the UAS.

2. NECESSARY SECURITY CAPABILITIES

Based on the results of the impact assessment, agencies must document how they will ensure the fulfillment of the minimum-security requirements listed below, with respect to the UAS to be acquired.

A. Access control requirements:

1. If personnel remotely access UAS ground control stations, agencies should require and enforce appropriate authentication at the identification and authentication levels, including multifactor authentication per NIST SP 800-63,[14] or any successor publication.

2. If the overall system impact level for availability is moderate or high, agencies should consider whether the UAS program should be managed in accordance with an IT

[12] National Institute of Standards and Technology (NIST), FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (2004), https://csrc.nist.gov/pubs/fips/199/final.
[13] *See* Pub. L. No. 107-347, § 208 (addressing privacy impact assessments); OMB Memorandum M-03-22.
[14] NIST SP 800-63-3, Digital Identity Guidelines, (last updated March 2, 2020, https://csrc.nist.gov/pubs/sp/800/63/3/upd2/final.

asset framework such as NIST SP 1800-5[15] or any successor publication.

B. Software and firmware update requirements:

1. Software and firmware updates should come only from the UAS manufacturer or a trusted (as determined by the authorizing official) third-party.

2. IT technology used for the installation and download of UAS software and firmware should be isolated from enterprise agency information systems.

3. If the overall system impact level for integrity is moderate or high, operators should conduct a file integrity check and test firmware or software updates prior to mission operations.

C. Data protection requirements:

1. To the extent practicable, UAS Federal mission-related data should be encrypted at rest and during the collection and transmittal of such information.

2. Sensitive data that is collected, stored, or processed by the UAS, or transmitted to or from it, should be cryptographically secured using approved and validated cryptographic algorithm and module.

3. Agencies should retain the ability to opt out of any uploading, downloading, or transmitting of UAS data that is not required by law or regulation. When uploading, downloading, or transmitting data is required by law or regulation, agencies should preserve the ability to choose with whom information is shared and where it is stored, to the greatest extent practicable.[16]

4. If the UAS stores or processes sensitive data, agencies should consider acquiring a UAS with remote security capabilities (e.g., remote wipe or lock). Ideally, the operator should be able to trigger these remote security capabilities without manufacturer involvement.

5. If the UAS stores or processes sensitive data operators should, consistent with applicable law, erase any Federal information with a moderate or high confidentiality designation that was collected by the UAS after each mission is completed.

6. If the overall system impact level for confidentiality is high, technical controls should be employed to disable data storage and transmission to non-approved systems.

---

[15] NIST, SP 1800-5, IT Asset Management (2018), https://doi.org/10.6028/NIST.SP.1800-5.
[16] Pub. L. No. 118-31, § 1829.

Appendix C: Exemptions

1. EXEMPTIONS UNDER SECTION 1829 OF THE ACT

If the head of an agency determines in writing with respect to a particular procurement or set of procurements that the agency cannot both satisfy the requirements outlined in Appendix B of this memorandum and obtain a UAS capable of fulfilling mission-critical performance requirements, then the procurement in question is exempt from the Appendix B requirements. Such an exemption is effective only if the agency head documents in writing, in addition to the determination described in the preceding sentence, the factual and logical basis for that determination and the following information:

(1) Date of determination;

(2) A description (including quantity and value) of the products covered; and

(3) The time period during which the exemption is valid, which may not exceed three years from the effective date.

An agency head may delegate the authority to make the determination required for an exemption to a Deputy Secretary or equivalent, but not to a lower-level official. Agencies must make documentation of exemptions available to OMB upon request, and also ensure that such documentation is both present in relevant system security plans and shared with acquisition officials for inclusion in relevant contract files.

2. EXEMPTIONS AND WAIVERS UNDER SECTIONS 1823, 1824, AND 1825 OF THE ACT

The Act establishes prohibitions on the acquisition or operation by Federal agencies, or using Federal funds, of UAS that were manufactured or assembled by certain foreign entities.[17] Sections 1823, 1824, and 1825 of the Act provide a number of exemptions from those prohibitions to specific agencies under identified circumstances. When an agency relies upon one of those exemptions to take an action that would otherwise be prohibited by the Act, the agency must prepare documentation that identifies the exemption and demonstrates that it applies. Such documentation shall be made available to OMB upon request.

In addition to exemptions, Sections 1823, 1824, and 1825 each contain a waiver provision that allows the head of an executive agency to waive the prohibition in each section on a case-by-case basis with the approval of the Director of the Office of Management and Budget ("the Director"), after consultation with the Federal Acquisition Security Council. To request OMB approval of a proposed waiver, agencies should use the waiver request template and submission instructions available at https://community-dc.max.gov/x/fAXSng.

[17] ASDA, §§ 1823-26. For agency procurements, these prohibitions have been incorporated into the Federal Acquisition Regulation. *See* 48 C.F.R. §§ 40.201-, 52.240-1.

In addition to receiving the Director's approval, an agency must notify Congress before waiving one of the Act's prohibitions. This notification must be provided to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability in the House of Representatives, and other appropriate congressional committees of jurisdiction. Agencies shall provide congressional notification of the intent to waive only after the Director has approved the waiver.

Appendix D: Prohibition on Procurement or Operation of Covered Unmanned Aircraft Systems Using Funds Provided Through a Grant, Cooperative Agreement, or Other Award

Pursuant to section 1825 of the American Security Drone Act of 2023 (Public Law 118-31), on or after December 22, 2025, the following prohibition applies to the use of funds provided through any Federal grant, cooperative agreement, or other award.

(1) ***Definitions.***
The terms "FASC-prohibited unmanned aircraft system" and "unmanned aircraft system" have the definitions provided in 48 C.F.R. § 40.201, or successor regulation.

(2) ***Prohibition.***
Pursuant to the prohibition in section 1825 of the American Security Drone Act of 2023 (Public Law 118-31), on or after December 22, 2025, except as provided in paragraphs (3) through (6) below, no Federal funds awarded through a grant or cooperative agreement, or otherwise made available, may be used by a recipient or subrecipient:

(i) To procure a FASC-prohibited unmanned aircraft system; or

(ii) In connection with the operation of a FASC-prohibited unmanned aircraft system.

(3) ***Department of Homeland Security, Department of Defense, Department of State, and the Department of Justice exemptions.***
The Secretary of Homeland Security, the Secretary of Defense, the Secretary of State, and the Attorney General are exempt from the restriction under paragraph (2) if the procurement or operation is required in the national interest of the United States and:

(i) is for the sole purposes of research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned aircraft system or counter-unmanned aircraft system technology;

(ii) is for the sole purposes of conducting counterterrorism or counterintelligence activities, protective missions, or Federal criminal or national security investigations, including forensic examinations, or for electronic warfare, information warfare operations, cybersecurity, or development of an unmanned aircraft system or counter-unmanned aircraft system technology; or

(iii) is an unmanned aircraft system that, as procured or as modified after procurement but before operational use, can no longer transfer to, or download data from, a covered foreign entity and otherwise poses no national security cybersecurity risks as determined by the exempting official.

(4) ***Department of Transportation and Federal Aviation Administration exemption.***
The Secretary of Transportation is exempt from the restriction under paragraph (2) if the operation or procurement is deemed to support the safe, secure, or efficient operation of the National Airspace System or maintenance of public safety, including activities carried

out under the Federal Aviation Administration's Alliance for System Safety of UAS through Research Excellence (ASSURE) Center of Excellence (COE) and any other activity deemed to support the safe, secure, or efficient operation of the National Airspace System or maintenance of public safety, as determined by the Secretary or the Secretary's designee.

(5) ***National Oceanic and Atmospheric Administration (NOAA) exemption.*** The Administrator of the National Oceanic and Atmospheric Administration (NOAA), in consultation with the Secretary of Homeland Security, is exempt from the restriction under paragraph (2) if the operation or procurement is necessary for the purpose of meeting NOAA's science or management objectives or operational mission.

(6) ***Waivers.*** The head of a Federal agency may waive the prohibition under paragraph (2) on a case-by-case basis:

(i) with the approval of the Director of the Office of Management and Budget, after consultation with the Federal Acquisition Security Council; and

(ii) upon notification to:

(a) the Committee on Homeland Security and Governmental Affairs of the Senate;

(b) the Committee on Oversight and Accountability in the House of Representatives; and

(c) other appropriate congressional committees of jurisdiction.