National Aeronautics and Space Administration
Washington, DC

Grant Information Circular (GIC)

GIC 26-04
06/2026

Unmanned Aircraft System Security Requirements

PURPOSE: To provide NASA grant and cooperative agreement applicants with a notice of forthcoming requirements pertaining to recipient-procured unmanned aircraft systems (UAS) that process, store, or transmit Federal information in accordance with Office of Management and Budget (OMB) memorandum M-26-02, *Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers*.

BACKGROUND: OMB memorandum M-26-02 requires NASA to apply appropriate safeguards for the protection of Federal information that is generated by or otherwise accessible to UAS, including those procured using NASA grant and cooperative agreement funds. To effectuate this requirement, NASA will conduct an impact assessment of UAS that process, store, or transmit Federal information utilizing Federal Information Processing Standards (FIPS) 199, or any successor publications. The impact assessment will determine whether the loss of confidentiality, integrity, or availability of information could be expected to result in low, moderate, or high potential impact on NASA operations, assets, or individuals.

NASA notices of funding opportunities (NOFOs) developed on or after the effective date of this GIC will include the clause in section A below, and applicants will be required to respond to the NOFO requirements if they intend to procure certain UAS using NASA grant or cooperative agreement funds. If NASA approves of the UAS procurement and issues an award, then the terms and conditions in section B will be applicable to the award. The impact assessment requirements in this GIC do not apply to recipient-procured UAS that will not process, store, or transmit Federal information.

Applicants and recipients are reminded of prohibitions on the use of Federal funds for the procurement and operation of covered UAS from covered foreign entities as described in section 1825 of the National Defense Authorization Act for Fiscal Year 2024 and Appendix B of the NASA Grant and Cooperative Agreement Terms and Conditions (GCAT) as well as International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) requirements as described in sections 16.7-16.9 of the NASA Grant and Cooperative Agreement Manual (GCAM).

GUIDANCE:

A. NOFO Requirements

NASA NOFO Omnibuses and NOFO Appendices will include the following clause, and grant and cooperative agreement applicants will be required to respond if they intend to procure a UAS that will process, store, or transmit Federal information .

[Begin clause]

Security Requirements for UAS Procured Using NASA Grant or Cooperative Agreement Funding

Background & Applicability

Office of Management and Budget (OMB) memorandum M-26-02, *Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers*, requires Federal agencies to apply appropriate safeguards for the protection of Federal information that is generated by or otherwise accessible to unmanned aircraft systems (UAS), including those procured using Federal grant and cooperative agreement (hereinafter "grant") funds.

Any grant issued under this NOFO that will fund the procurement of UAS that process, store, or transmit Federal information is required to adhere to the security requirements described below. Applicants that intend to procure such UAS must clearly and explicitly describe the intended procurement in their budget and budget narrative and describe the intended procurement in the Scientific/Technical/Management Plan section of their proposal or other applicable section as described in a NOFO omnibus or NOFO appendix. After proposal submission, NASA may request that additional information pertaining to the proposed UAS procurement be provided so that NASA may conduct an impact assessment per requirements in M-26-02.

For the purposes of this NOFO, "Unmanned aircraft system" has the definition found in Title 48 of the Code of Federal Regulations (CFR), section 40.201, Definitions: "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12))."

"Federal information" is defined as "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form." This definition of "federal information" is derived from OMB Circular A-130, *Managing Information as a Strategic Resource*.

Security Requirements for UAS

Applicants proposing to use NASA grant funds to procure UAS that will process, store, or transmit Federal information must describe how they will manage the UAS in accordance with the information security requirements listed below. Applicants must also describe how they will develop a risk-based approach to applying these requirements to procurement solicitations to potential UAS vendors.

1. **Access Control Requirements**

    a. If personnel will remotely access UAS ground control stations, applicants should

require and enforce appropriate authentication at the identification and authorization levels, including multifactor authentication per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identify Guidelines, or any successor publication.

b. If the overall system impact level for availability is moderate or high, applicants should consider whether the UAS program should be managed in accordance with an IT asset framework such as NIST SP 1800-5, IT Asset Management, or any successor publication.

2. Software and Firmware Update Requirements

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

b. IT technology used for the installation and download of UAS software and firmware should be isolated from the applicant's information systems.

c. 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.

3. Data Protection Requirements

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

b. 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.

c. NASA retains 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, NASA will preserve the ability to choose with whom information is shared and where it is stored, to the greatest extent practicable. See National Defense Authorization Act for Fiscal Year 2024 (Pub. L. No 118-31 § 1829) for more information.

d. If the UAS stores or processes sensitive data, applicants 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.

e. 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.

f. 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.

For each intended UAS procurement, a description of the types of information that may be stored in, processed by, or transferred to or from the UAS must be provided. Information that must be provided includes, but is not limited to:

- **Telemetry and flight data**: Real-time data (e.g., altitude, speed, location) regarding the UAS's status.
- **Audio/visual/sensor feed**: Imagery or sensor data (e.g., Electro-optical/infrared, radar) gather by the UAS.
- **Operational information**: Flight plans, mission plans, and operator information.
- **Operational log data**: System logs, flight logs, and configuration data used for maintenance and operational analysis.
- **User/mission data**: Data stored or transmitted specifically for the mission objective.
- **Navigation Aids (NAVAIDS) data**: Information used for positioning, including GPS or inertial navigation data.

[End clause]

B. Terms and Conditions

If a grant or cooperative agreement recipient will procure a UAS using NASA funds that will process, store, or transmit Federal information, then the following term and condition will apply:

[Begin term and condition]

Security Requirements for UAS Procurements

Office of Management and Budget (OMB) memorandum M-26-02, *Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers*, requires Federal agencies to apply appropriate safeguards for the protection of Federal information that is generated by or otherwise accessible to unmanned aircraft systems (UAS), including those procured using Federal grant and cooperative agreement (hereinafter "award") funds. These terms apply to any recipient of NASA award funds used to procure unmanned aircraft systems (UAS) that process, store, or transmit Federal information.

For the purposes of this award, "Unmanned aircraft system" has the definition found in Title

48 of the Code of Federal Regulations (CFR), section 40.201, Definitions: "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12))."

"Federal information" is defined as "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form." This definition of "federal information" is derived from OMB Circular A-130, *Managing Information as a Strategic Resource*.

This term and condition is only applicable to proposers that were required to respond to the "Security Requirements for UAS Procured Using NASA Grant or Cooperative Agreement Funding" notice of funding opportunity clause.

Recipient Requirements

1. Recipients that intend to procure UAS that will process, store, or transmit Federal information must adhere to the information security requirements for that UAS as described in the proposal associated with this award and must ensure the security requirements will be incorporated into procurement solicitations of UAS under this award. As applicable, those security requirements include:

    a. **Access Control Requirements**

        i. If personnel will remotely access UAS ground control stations, applicants should require and enforce appropriate authentication at the identification and authorization levels, including multifactor authentication per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identify Guidelines, or any successor publication.

        ii. If the overall system impact level for availability is moderate or high, applicants should consider whether the UAS program should be managed in accordance with an IT asset framework such as NIST SP 1800-5, IT Asset Management, or any successor publication.

    b. **Software and Firmware Update Requirements**

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

        ii. IT technology used for the installation and download of UAS software and firmware should be isolated from the applicant's information systems.

        iii. 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**

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

ii. 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.

iii. NASA retains 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, NASA will preserve the ability to choose with whom information is shared and where it is stored, to the greatest extent practicable. See National Defense Authorization Act for Fiscal Year 2024 (Pub. L. No 118-31 § 1829) for more information.

iv. If the UAS stores or processes sensitive data, applicants 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.

v. 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.

vi. 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.

2. Recipients must receive prior written approval from a NASA Grant Officer before procuring UAS that will process, store, or transmit Federal information if the UAS was not described in the proposal and budget for this award.

[End term and condition]

EFFECTIVE DATE*:* **July 15, 2026**, and shall remain in effect until canceled or superseded

REGULATION OR TERMS AND CONDITIONS CHANGES: Yes. See section B above.

CONTACTS:

- **OP**: Office of Procurement, Grant Operations Management, hq-dl-grant-operations-management@mail.nasa.gov

- **OCIO**: Office of the Chief Information Officer, Cybersecurity Standards and Engineering Office, Michael Powers, Michael.L.Powers@nasa.gov

January 31, 2024

TO: All Center Directors
Jet Propulsion Laboratory
Aeronautics Research Mission Directorate
Exploration Systems Development Mission Directorate
Science Mission Directorate
Space Operations Mission Directorate
Space Technology Mission Directorate
NASA Shared Services Center

FROM: Associate Administrator, Mission Support Directorate

SUBJECT: Unmanned Aircraft Systems (UAS) Policy Update

This letter provides an interim update to NASA's policy on Unmanned Aircraft Systems (UAS) so as to fully comply with the prohibitions and requirements set forth in the American Security Drone Act (ASDA) of 2023. This interim policy update on NASA UAS will be formally incorporated in the planned NASA Procedural Requirement (NPR) 7920.

The ASDA of 2023 was enacted in Sections 1821 to 1833 of the FY 2024 National Defense Authorization Act (NDAA), which became law on December 22, 2023. Except for specifically exempted entities, the ASDA prohibits executive agencies from acquiring, funding, and operating UAS manufactured or assembled by covered entities that are defined in the statute. Covered UAS includes associated elements related to the collection and transmission of sensitive information (consisting of communication links and the components that control the unmanned aircraft) that enable the operator to operate the aircraft in the National Airspace System. Although the ASDA does not provide a comprehensive definition of "associated elements," it requires the Federal Acquisition Security Council, in coordination with the Secretary of Transportation, to develop and update a list of associated elements. Previous examples of certain UAS components that could constitute "associated elements" can be found in Section 848(a)(1-2) of the 2020 NDAA and Section 6(b-c) of Executive Order 13981.

In compliance with the stipulations of the ASDA, until its sunset on December 22, 2028, the following requirements are NASA policy and apply to the Agency in its entirety, including NASA programs, projects, and activities involving covered UAS:

(1) Effective Immediately, NASA shall not procure any covered UAS that is manufactured or assembled by a covered foreign entity (ASDA Sec. 1823).

(2) NASA offices, employees, contractors, and grantees shall, by the end of FY 2025, stop operating and disposition any covered UAS (ASDA Sec. 1824).

(3) By the end of FY 2025, NASA funds, awarded through a contract, grant, or cooperative agreement, or otherwise made available, shall not be used to procure or operate a covered UAS (ASDA Sec. 1825).

(4) Effective immediately, Government-issued Purchase Cards shall not be used to procure any covered UAS from a covered foreign entity (ASDA Sec. 1826).

(5) Covered UAS and their disposition shall be accounted for in NASA's personal property accounting system (ASDA Sec. 1827).

The following Agency policy guidance previously published also remain in effect:

(1) March 3, 2015 UAS Policy Amplification by Aircraft Management Division (AMD) that delegated the acquisition of UAS below the Agency's Capital Asset Threshold to Center Directors.

(2) October 23, 2018 UAS Policy Amplification by AMD that implemented the 2015 Presidential Memorandum regarding the domestic use of UAS, as well as recommendations from 2017 Office of Inspector General (OIG) report on NASA UAS.

(3) March 01, 2018 Small UAS (SUAS) Cyber Security Policy issued by the Office of the Chief Information Officer to mitigate cyber security risks posed by sUAS operations, and in particular sUAS manufactured by Da-Jiang Innovations (DJI).

Questions concerning this latest policy update should be directed to the Director of the Aircraft Capability Management Office.

Robert Gibbs