

AIR FORCE RESEARCH LABORATORY (AFRL)
ADDENDUM TO DOD R&D GENERAL TERMS AND CONDITIONS
APRIL 2026

Applicability

This award is subject to the DoD Research and Development (R&D) General Terms and Conditions (Ts&Cs), which are hereby incorporated into this award by reference. The DoD R&D General Ts&Cs are located at: <https://www.onr.navy.mil/work-with-us/manage-your-award/manage-grant-award/grants-terms-conditions>.

This AFRL document is a supplement to the DoD R&D General Ts&Cs. It is aligned with the structure and format of the DoD R&D General Ts&Cs. To understand the entire AFRL requirement for a given article, the DoD R&D General Ts&Cs must be read in tandem with this document. This document uses plain language as described in the preamble to the DoD R&D General T&Cs.

The Division III portion of this document is the AFRL Addendum to the DoD R&D Ts&Cs, which provides additional content relevant to AFRL awards for the “RESERVED” sections of specified articles from the DoD R&D General T&Cs. If a block appearing immediately to the left of the article or Section(s)/ Subsection(s) is checked, it is applicable to your award. If a block remains unchecked, you must continue to comply with the DoD General R&D T&Cs for that Section/Subsection. If Section(s) or Subsection(s) are not specifically addressed in this document, the DoD R&D General T&Cs Section(s)/Subsection(s) remain in effect and are unchanged for your award.

The Division II portion of this document is comprised of the AFRL Award-Specific T&Cs subject to the DoD R&D General Terms and Conditions.

Order of Precedence

Any inconsistencies in the requirements of this award shall be resolved as specified in the DoD General R&D Terms and Conditions, Order of Precedence. In case of disagreement with any requirements of this award, you shall contact the AFRL Grants Officer (AFRL GO) to resolve the issue. You shall not assess any costs to the award or accept any payments until the issue is resolved.

AFRL Addendum to DoD R&D General Terms and Conditions

Part 1: Financial And Program Management (FMS Articles)

FMS Article II. Payments.

[X] Section C. Electronic funds transfer and other payment procedural instructions or information.

1. Electronic funds transfer.

[X] a. Electronic Funds Transfer Information. All payments will be made by funds transfers to the bank account registered in System for Award Management (SAM) at <https://www.sam.gov/SAM/>. You must maintain the currency of information about yourself in SAM, including information necessary to facilitate payment via Electronic Funds Transfer (EFT). We cannot be held responsible for any misdirection or loss of payment which occurs as the result of your failure to maintain correct/current EFT information within your SAM registration.

[X] b. Electronic Payment Request Instructions. You must submit payment requests (advance or reimbursement) through the Wide Area Workflow (WAWF) page, located within the Procurement Integrated Enterprise Environment (PIEE) system at <https://wawf.eb.mil>. Within WAWF, the following codes and information are required to initiate the "Grant Voucher" and assure successful flow of the payment request. To learn how to electronically submit and take action on WAWF documents through simulations and step-by-step procedures, visit the PIEE Procurement Integrated Enterprise Environment Web Based Training Main Menu at <https://pieetraining.eb.mil/wbt/>, and select WAWF. For a demonstration of a Vendor creating a Grant Voucher document, go to <https://pieetraining.eb.mil/wbt/wawf/VendorCreateGrantDocument.pdf>. This document explains the steps to be followed, the Create From Template option and an explanation of a Grant Voucher.

WAWF FIELD

DATA INPUT

CONTRACT NUMBER: See Block 1 of Award Form
DOCUMENT TYPE: SF270 Grant Voucher
DELIVERY ORDER : N/A
CAGE CODE : See Block 13 of Award Form
ISSUE BY DODAAC: See Block 11 of Award Form
ADMIN DODAAC: See Block 12 of Award Form
GOVERNMENT PROGRAM OFFICER: See Address Information section
PAY OFFICE DODAAC: See Block 14 of Award Form
GRANT APPROVER DODAAC: See Block 11 of Award Form

[X] c. Questions for the Payment Office. Most payments are made within 30 calendar days as described at 2 CFR 200.305. Recipients can check payment processing status directly through the WAWF PIEE or my Invoice applications (<https://piee.eb.mil/>). The customer service telephone number for Defense Finance and Accounting Services (DFAS) is 1-800-756-4571 Option 4, then select the option associated with the pay office indicated in Block 14 of the Award Form. Questions concerning specific payments should be directed to the Defense Finance and Accounting Service (DFAS) at <https://www.dfas.mil/dfas/AskDFAS/>.

[X] d. Instructions for the Payment Office. The payment office must make payment by using the oldest fiscal year appropriations first, exhausting all funds in the previous fiscal year before disbursing from the next fiscal year. In the event there is more than one ACRN associated with the same fiscal year, payment will be made in sequential ACRN order within the award, exhausting all funds in the previous ACRN before paying from the next ACRN using the following sequential order: alpha/alpha; alpha/numeric; numeric/alpha; and numeric/numeric ACRN sequence unless otherwise specified in the award-specific terms and conditions.

[] e. Cost sharing. If your award contains a cost-sharing arrangement, each request for payment shall include the total costs incurred and the amounts of your cost share and the Government cost share. We agree to reimburse you no more than the Government cost share percentage of all requests submitted except the final payment request. The final payment will reflect the percentage representing the balance of Government cost share.

[X] f. Final payment. Final payment may be withheld until Performance Report(s), Final Financial Report (SF425), Final Patent Report (DD882), and any other deliverables are delivered and accepted.

2. Other Payment Procedural Instructions or Information.

☐ a. Preferred method of payment by Wire Transfer via ITS.gov has been selected and authorized by the Awardee.

☐ a. Payment – Predetermined Payment Schedule

(1) Payment will be made immediately upon receipt of funds in accordance with the Incremental Funding Periods table.

FMS Article IV. Revision of budget and program plans.

☒ Section B. Revisions requiring prior approval from the AFRL GO.

1. Non-construction activities.

e. You must request prior approval from the AFRL GO for any of the following program or budget revisions in non-construction activities:

Period of Performance Extensions. We require prior written approval to extend the period of performance, without additional funds, beyond the expiration date of the grant. We only grant no-cost extensions (NCE) when they are truly warranted and properly documented. For an extension to be granted, all NCE requests must be received at least 30 days prior to the expiration of the grant's period of performance. An award modification must be issued and signed by the AFRL GO for the NCE to be in effect.

The NCE request must include:

(1) Request letter from the business office on University's or Institute's letterhead.

(2) Compelling reason(s) for the extension beyond using unexpended balances.

(3) Original end date and requested extension length.

(4) SF 425 Federal Financial report showing the unexpended funds remaining or the most recent SF 270

(5) Statement indicating all required previous annual reports have been provided to AFOSR.

In no event will the period of performance be extended merely for the purpose of using unobligated balances or exclusively for the purpose of additional time to submit reports.

☒ All NCE requests must be submitted through the following website:

https://afosr.gov1.qualtrics.com/jfe/form/SV_4UcsVbwxSaic8S. AFOSR will no longer accept NCE requests via email. All requests that are submitted through other avenues will have to be re-routed through the above website.

☐ All NCE requests must be forwarded to the Government Technical Representative / Program Office and AFRL GO with the required information listed above.

3. Funding transfers between construction and non-construction activities.

☐ RESERVED

☒ Section C. Pre-award costs, carry forward of unobligated balances, and one-time no-cost extensions.

3. Pre-award Costs. Pre-award costs exceeding 90 days before the start of the period of performance as stated on Block 16 of the Award Form are authorized if approved in writing by the AFRL GO prior to grant award. In no event is the Government obligated to reimburse you for expenditures in excess of the negotiated budget or the total funds allotted by the Government to this agreement, whichever is the lesser of the two amounts.

☒ Section D. Procedures.

2. Additional procedural instructions for prior approvals. Revised budgets, when required, must be submitted on the SF 424 "Research and Related Budget" form (part of the SF 424 Research and Related (R&R) family) or in the same format as your original budget submission unless directed otherwise by the AFRL GO or cognizant administration office (AGO).

FMS Article VI. Cost sharing or matching.

☐ Section A. Required cost sharing or matching.

2. You must obtain AFRL GO prior approval if you wish to:

b. Substitute alternative cost sharing or matching contributions in lieu of specific contributions included in the approved budget.

☐ RESERVED

Part 2: Property Administration (PROP Articles)

PROP Article I. Title to property.

☐ Section B. Property trust relationship.

2. Notices of record. RESERVED

Part 3: Procurement (PROC Articles)

PROC Article III. Procurement standards for institutions of higher education, nonprofit organizations, local governments, Indian tribes and for-profit entities.

☒ Section A. General procurement standards.

2. You must do business only with responsible contractors who are able to perform, as described in OMB guidance in 2 CFR 200.318(h). Related to that, you must comply with restrictions on awarding procurement transactions to excluded or disqualified parties and other requirements specified by OMB guidelines on non-procurement debarment and suspension at 2 CFR part 180, as implemented 37 by DoD at 2 CFR part 1125.

☐ Section J. Bonding requirements. RESERVED

PROC Article IV. Contract provisions for recipient procurements.

Section B. Contract provisions for national policy requirements.

☐ 2. Wage Rate Requirements (Construction). RESERVED

☐ 3. Copeland Act prohibition on kickbacks. RESERVED

Part 4: Financial, Programmatic, and Property Reporting (REP Articles)

REP Article I. Performance management, monitoring, and reporting.

☒ Section B. Frequency, reporting periods, and due dates for interim performance reports.

1. The instructions applicable to your award are in the Reporting Information section of the grant. The AFRL Awarding Office may waive any interim performance report required by this section only if there is an alternative source for the information that the reports provide per 2 CFR 1134.110 (b)(1).

☒ Section C. Due date and reporting period for final performance report: See the Reporting Information section of the grant. The final performance report should cover the entire period of performance of the grant including any exercised options.

☒ Section F. Performance reporting procedures.

For additional information pertaining to the form, format, and data elements described below, view the National Science Foundation Website as follows: Research Performance Progress Report (RPPR) | NSF - National Science Foundation. This website lists a Format for Use and Submission of Interim and Final Research Performance Progress Reports (RPPR) and the Federal Register Notice Announcing the format for use in submission of Interim and Final RPPR.

c. Other Requirements.

1. Interim Performance Reports.

a. Form and Format. You must submit performance reports using OMB-approved Government wide standard information collections when providing performance information (including performance progress reports, Research Performance Progress Report (RPPR), or such future collections as may be approved by OMB). Recipient shall submit RPPR in accordance with this article and 2 CFR 200.329.

b. Data Elements. Your Interim Performance Reports must detail technical progress to date during the reporting period. Address the following performance reporting requirements:

i. Accomplishments:

(a) A comparison of your actual accomplishments to the objectives of the Federal award established for the period. Where the accomplishments of the Federal award can be quantified, a computation of the cost (for example, related to units of accomplishment) and/or performance trend data and analysis may be included in your report(s).

(b) The reasons why established goals were not met, if appropriate.

(c) Additional pertinent information including, when appropriate, analysis and explanation of cost overruns or high unit costs.

ii. Real Property: Status of real property acquired or improved under the award.

iii. Significant Developments. Events may occur between the scheduled performance reporting dates that have a significant impact upon the supported activity. In such cases, the non-Federal entity must inform the Federal awarding agency or pass-through entity as soon as the following types of conditions become known:

(a) Problems, delays, or adverse conditions which will materially impair the ability to meet the objective of the Federal award. This disclosure must include a statement of the action taken, or contemplated, and any assistance needed to resolve the situation.

(b) Favorable developments which enable meeting time schedules and objectives sooner or at less cost than anticipated or producing more or different beneficial results than originally planned.

iv. Participants and Other Collaborating Organizations. In accordance with the National Defense Authorization Act for Fiscal Year 2020, you must include in your quarterly/final reports a list of all participants and other collaborating organizations in a section titled "Participants and Other Collaborating Organizations." You are reminded IAW 2 CFR 200.308, any changes to key personnel require AFRL GO approval prior to change implementation. Failure to comply with these items can result in corrective actions as prescribed in 2 CFR 200.339.

v. Patent/Invention Information. Include any new discoveries, inventions, or patent disclosures during this reporting period (if none, report none).

vi. Reports SHALL be submitted in English.

2. Final Performance Report.

a. Form and Format. You must submit performance reports using OMB-approved Government wide standard information collections when providing performance information (including performance progress reports, Research Performance Progress Report (RPPR), or such future collections as may be approved by OMB). Recipient shall submit RPPR in accordance with this article and 2 CFR 200.329.

i. Standard Form (SF) 298: Prepare the Cover/Title Page by completing the SF 298, Report Documentation Page. In Item 14 include a 100 to 200 word abstract summarizing technical progress during the reporting

period. Style is to be third person singular using past tense. Jargon, special symbols or notations, subscripts, mathematical symbols or foreign alphabet letters are not permitted. All pages should be of good quality for copying purposes. The form and instructions are available at <https://www.gsa.gov/forms-library/report-documentation-page>. However, Block 12a. of the SF 298 should be completed with the distribution statements described herein. If you do not agree with that distribution/availability, you should contact the AFRL GO.

ii. ANSI/NISO: The report shall be prepared in accordance with American National Standard Institute document ANSI/NISO Z39.18-2005 (R-2010), Scientific and Technical Reports - Elements, Organization, and Design which may be obtained from:

NISO Press Fulfillment Center
PO Box 451
Annapolis Junction MD 20701-0451
<http://www.niso.org>

iii. You may use your own format for the final report, but it must include the same data elements used for interim performance reports, excluding the patent/invention information, as well as include the content listed above and indicate on the cover page of the report that it is the final performance report.

b. Data Elements. Your Final Performance Report will provide a comprehensive, cumulative and substantive summary of the progress and significant accomplishments achieved during the period covered by this agreement. Address each of the data elements listed for the interim performance reports above excepting Patent/Invention Information , as appropriate.

c. Other Requirements.

i. Notice: All publications shall contain the notices included in the Article entitled, "Publishing Project Results" (located in the second portion of this document, the AFRL Award-Specific Ts&Cs Section). Publications may be attached as appendices.

ii. Reports SHALL be submitted in English.

3. Distribution Statement

In addition to any other required legend, mark all data delivered under this award with the following distribution statement that indicates to whom data may be distributed:

DISTRIBUTION A. Approved for public release: distribution unlimited.

4. Interim and Final Performance Report - Submission: See the Reporting Information section of the grant. AFOSR prefers Performance Reports to be submitted electronically; however, if the awardee does not have access to electronic means, send paper copies of Performance Reports to the Government Technical Representative / Program Office listed in Address Information section.

REP Article II. Financial reporting.

[X] Section A. Required reporting form, format, or data elements for interim and final financial reports.

1. Interim reports for awards with advanced or a predetermined payment schedule are required. You must submit the Federal Financial Report [currently the SF 425; only Fields 1 through 9, 10.a through 10.c, 12 (as needed)] or successor OMB-approved Government wide standard data elements for information collection.
2. Interim reports for awards with cost reimbursement are not required.
3. Final reports. You must submit the Federal Financial Report (currently the SF 425) or successor OMB-approved Government wide standard data elements for information collection for all awards. If you are a domestic institution of higher education, you must complete the optional fields 11.a through 11.f, "Indirect Expense" on the final Federal Financial Report that you submit after the end of the project period under the award.

[X] Section B. Financial reports: frequency, reporting periods, and due dates. – See the Reporting Information section of the grant. The final financial report should cover the entire period of performance of the grant including any exercised options.

1. Awards with advanced payment or a predetermined payment schedule. – See the Reporting Information section of the grant for interim financial reporting requirements and dates.
2. Awards with cost reimbursement. – See the Reporting Information section of the grant. You must submit the Final Financial Report only. Your report is due 90 calendar days after the reporting period.

[X] Section E. Where and how to submit financial reports. – See the Reporting Information section of the grant.

REP Article III. Reporting on property.

[] Section A. Real property

1. Periodic status reports.
 - a. Frequency and duration of reporting requirement. See REP Article I instructions contained herein. RESERVED
 - b. Due dates. See REP Article I instructions contained herein. RESERVED
 - c. Other submission instructions. See REP Article I instructions contained herein. RESERVED

Part 5: Other Administrative Requirements (OAR Articles)

[X] OAR Article I. Submitting and maintaining recipient information

Federal award recipients are required to update entity, recipient integrity, and performance information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis. This update is accomplished by entering the required information in the System for Award Management (SAM) database at <https://www.sam.gov>. Recipient updates must include, but are not limited to, entity changes, any mandatory disclosures required by 2 CFR 200.113, and/or Appendix XII to 2 CFR Part 200 -

Award Term and Condition for Recipient Integrity and Performance Matters, incorporated here by reference. This requirement continues for the entire Grant relationship.

OAR Article IV. Claims, disputes and appeals.

[X] Section A. Definitions.

2. Grant Appeal Authority. Director of Contracting, HQ AFMC/PK.

OAR Article V. Collection of amounts due.

[X] Section A. Establishing a debt.

1. Any amount paid to you in excess of the amount to which you are determined to be entitled under the terms and conditions of this award constitutes a debt to the Federal Government.

2. The grants officer will attempt to resolve any claim of your indebtedness arising out of this award by mutual agreement.

3. If the grants officer fails to resolve the claim in that manner, you will receive a written notice of the grants officer's decision formally determining the debt, as described in paragraph B.2 of OAR Article IV. The notice will describe the debt, including the amount, name and address of the official who determined the debt, and a copy of that official's determination.

Part 6: Subawards (SUB Articles)

SUB Article V. Property requirements for subawards.

[X] Section B. Title to property.

Subawards to institutions of higher education, nonprofit organization, States, local governments, Indian tribes, or for-profit entities.

b. Exceptions. For a subaward to conduct basic or applied scientific research with a nonprofit institution of higher education or nonprofit organization whose primary purpose is conducting scientific research, you must include terms and conditions in that subaward that allow the title to all equipment and supplies acquired under that subaward and charged as direct costs to the project or program to vest with the subrecipient upon acquisition subject only to the following three conditions related to equipment:

i. The subrecipient uses the equipment for the authorized purposes of the project or program until the property is no longer needed for those purposes.

ii. The subrecipient manages the equipment as provided in PROP Article II of these general terms and conditions. This includes maintaining property records that include the percentage representing the Federal share of total project costs under the award to you (the recipient) under which the subrecipient acquired the exempt property, so that the subrecipient may deduct the Federal share if it wishes to use the property in future contributions for cost sharing or matching purposes on Federal awards. When

both your award with the DoD Component has cost sharing requirements and your subaward allows for the purchase of exempt property, you must include in that subaward the percentage representing the Federal share of total project costs to enable the subrecipient's compliance with this provision.

iii. AFRL reserves the right to transfer title to the equipment to another entity if the Principal Investigator of a subrecipient relocates his or her research program to that entity. If AFRL elects to exercise its right to transfer the title of equipment, AFRL will contact the recipient to discuss the transfer.

b. Exceptions. RESERVED

Part 7: National Policy Requirements (NP Articles)

NP Article I. Nondiscrimination national policy requirements.

[] Section B. Other nondiscrimination requirements. RESERVED

NP Article II. Environmental national policy requirements.

[] Section B. Other environmental requirements. RESERVED

NP Article III. National policy requirements concerning live organisms.

Section C. Other requirements concerning live organisms.

1. With respect to the provisions in general terms and conditions for Section A of this article:

[] a. Section A.1, Human Subjects. Failure to comply with the applicable requirements of NP Article III. Section A.1. may result in the DoD Component's use of remedies, e.g., wholly or partially terminating or suspending the award, temporarily withholding payment under the award pending correction of the deficiency or disallowing all or part of the cost of the activity or action (including the Federal share and any required cost sharing or matching) that is not in compliance. Department of Defense Human Research Protection Official (HRPO) must perform an administrative review of the research and issue concurrence before the activities that involve human subjects can begin (e.g., human subject recruitment and related data collection). Language regarding HRPO review requirement must flow from the prime to any subawardees performing Human Subject research.

[] b. Section A.2., Animals. Recipients must comply with applicable provisions of Department of Agriculture rules at 9 CFR parts 1-4 and DoD Instruction 3216.1, which implement the Laboratory Animal Welfare Act of 1966 (7 U.S.C. 2131-2156) and provide for humane transportation, handling, care, and treatment of animals used in research, experimentation, testing, or training under this award. Recipients may not begin any animal work under the award that the awarding DoD Component has not reviewed and approved in advance, as specified in paragraph 2.d of Enclosure 3 to DoD Instruction 3216.1. Recipient's animal care programs must meet the standards set forth in the National Academy of Sciences publication "Guide for the Care and Use of Laboratory Animals" (eighth edition, 2011, which may be found currently at <http://www.nap.edu/catalog/12910/guide-for-the-care-and-use-of-laboratory-animals-eighth>). Recipients must immediately identify to us, as the Federal awarding agency, any potential impact that Recipients find this award may have on endangered species, as defined by the Endangered Species Act of 1973, as amended ("the Act," 16 U.S.C. 1531-1543), and implementing regulations of the Departments of the Interior (50 CFR parts 10-24) and Commerce (50 CFR parts 217-

227). Recipients also must provide any help the Federal awarding agency may need to comply with 16 U.S.C. 1536(a) (2). This is not in lieu of responsibilities Recipients have to comply with provisions of the Act that apply directly to Recipients as a U.S. entity, independent of receiving this award.

[] 2. Biosafety and Biosecurity Requirements: You must ensure compliance with standards meeting at least the minimum applicable requirements of the current edition of Centers for Disease Control and Prevention, "Biosafety in Microbiological and Biomedical Laboratories (BMBL)," and National Institutes of Health, "The NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules (NIH Guidelines)." Information concerning noncompliance with these requirements or any significant research-related incidents shall be provided to the Government Technical Representative / Program Office in a timely manner, after notification to the applicable safety committee or CDC or NIH.

[] 3. Research Involving Recombinant Nucleic Acid (rDNA) or Synthetic Nucleic Acid Molecules. You must not begin performance of research within the scope of "The NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules (NIH Guidelines)," until you receive notice from the AFRL GO that AFRL has reviewed and accepted your documentation. See most current information at https://osp.od.nih.gov/wp-content/uploads/Investigator_Brochure_Recombinant_DNA_2021.pdf?highlight=%22Recombinant%22&rt=MnwxfhJIY29tYmluYW50fDE3NDY3MTc4NTM&rt_nonce=8fd2335c87. In order for AFRL to accomplish that review, you must provide the AFRL GO, generally as part of your original proposal prior to award, sufficient documentation to enable the review that includes:

A written statement that your entity is in compliance with NIH Guidelines. This statement should be made by an official of the institution other than the Principal Investigator and should be on university or company letterhead.

Evidence demonstrating that your proposed research protocol has been approved by an Institutional Biosafety Committee (IBC); and a copy of the Department of Health and Human Services (DHHS) Letter of Approval of the IBC, or the most recent letter from DHHS stating that the IBC is in compliance with the NIH Guidelines.

You will not receive a separate approval for your proposed research under this paragraph. If you received the award based on a proposal including the two aforementioned items, you can assume the AFRL GO has accepted that documentation. If you add such research later, you will have to provide the two items of documentation listed above and a revised proposal. If this research is approved, you will receive a modification incorporating the revised proposal.

For research involving countries outside the United States, if the host country has established rules for the conduct of recombinant or synthetic nucleic acid molecule research, then the research must be in compliance with those rules. If the host country does not have such rules, the proposed research must be reviewed and approved by an NIH-approved IBC or equivalent review body and accepted in writing by an appropriate national governmental authority of the host country. The safety practices that are employed abroad must be reasonably consistent with the NIH Guidelines.

[] 4. RESERVED

NP Article IV. Other national policy requirements.

Section A. Cross-Cutting requirements.

[X] 3. Lobbying.

a. You must comply with the restrictions on lobbying in 31 U.S.C. 1352, as implemented by DoD at 32 CFR part 28, and submit all disclosures required by that statute and regulation.

b. You must comply with the prohibition in 18 U.S.C. 1913 on the use of Federal funds, absent express Congressional authorization, to pay directly or indirectly for any service, advertisement or other written matter, telephone communication, or other device intended to influence at any time a Member of Congress or official of any government concerning any legislation, law, policy, appropriation, or ratification.

c. If you are a nonprofit organization described in section 501(c)(4) of title 26, United States Code (the Internal Revenue Code of 1968), you may not engage in lobbying activities as defined in the Lobbying Disclosure Act of 1995 (2 U.S.C., chapter 26). If we determine that you have engaged in lobbying activities, we will cease all payments to you under this and other awards and terminate the awards unilaterally for material failure to comply with the award terms and conditions.

[X] 4. Officials not to benefit. You must comply with the requirement that no member of Congress shall be admitted to any share or part of this award, or to any benefit arising from it, in accordance with 41 U.S.C. 6306

[X] 7. Fly America Act. You must comply with the International Air Transportation Fair Competitive Practices Act of 1974 (49 U.S.C. 40118), commonly referred to as the "Fly America Act," and implementing regulations at 41 CFR 301-10.131 through 301-10.143. The law and regulations require that U.S. Government financed international air travel of passengers and transportation of personal effects or property must use a U.S. Flag air carrier or be performed under a cost-sharing arrangement with a U.S. carrier, if such service is available.

[X] 9. Research Misconduct

You must comply with requirements concerning research misconduct in Enclosure 4 to DoD Instruction 3210.7, "Research Integrity and Misconduct." The Instruction implements the Governmentwide research misconduct policy that the Office of Science and Technology Policy published in the Federal Register (65 FR 76260, December 6, 2000, available through the U.S. Government Printing Office web site:

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/321007p.pdf>

In accordance with Enclosure 4 to DoD Instruction 3210.7, "Research Integrity and Misconduct" paragraphs E4.1.5 through E4.1.7 (available at:

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/321007p.pdf?ver=2019-10-24-135242-857>), required notifications shall be sent to afrl.afosr.jag@us.af.mil.

[X] 16. Trafficking in persons. You must comply with requirements concerning trafficking in persons specified in the award term at 2 CFR 175.15(b), as applicable

[] 19. Do Not Contract with the Enemy (2 CFR 183)

Prescription: 2 CFR 183.10 Applicability

(a) This part applies only to grants and cooperative agreements that are expected to exceed \$50,000 and that are performed outside the United States, including U.S. territories, and that are in support of a contingency operation in which members of the Armed Forces are actively engaged in hostilities. It does not apply to the authorized intelligence or law enforcement activities of the Federal Government.

(b) All elements of this part are applicable until the date of expiration as provided in law.

Award Terms for Never Contract With the Enemy (Appendix A to Part 183)

Federal awarding agencies may include the following award terms in all awards for covered grants and cooperative agreements in accordance with Never Contract with the Enemy:

Term 1

Prohibition on Providing Funds to the Enemy

(a) The recipient must—

(1) Exercise due diligence to ensure that none of the funds, including supplies and services, received under this grant or cooperative agreement are provided directly or indirectly (including through subawards or contracts) to a person or entity who is actively opposing the United States or coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities, which must be completed through 2 CFR 180.300 prior to issuing a subaward or contract and;

(2) Terminate or void in whole or in part any subaward or contract with a person or entity listed in SAM as a prohibited or restricted source pursuant to subtitle E of Title VIII of the NDAA for FY 2015, unless the Federal awarding agency provides written approval to continue the subaward or contract.

(b) The recipient may include the substance of this clause, including paragraph (a) of this clause, in subawards under this grant or cooperative agreement that have an estimated value over \$50,000 and will be performed outside the United States, including its outlying areas.

(c) The Federal awarding agency has the authority to terminate or void this grant or cooperative agreement, in whole or in part, if the Federal awarding agency becomes aware that the recipient failed to exercise due diligence as required by paragraph (a) of this clause or if the Federal awarding agency becomes aware that any funds received under this grant or cooperative agreement have been provided directly or indirectly to a person or entity who is actively opposing coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities.

(End of term)

Term 2

Additional Access to Recipient Records

(a) In addition to any other existing examination-of-records authority, the Federal Government is authorized to examine any records of the recipient and its subawards or contracts to the extent necessary to ensure that funds, including supplies and services, available under this grant or cooperative agreement are not provided, directly or indirectly, to a person or entity that is actively opposing United States or coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities, except for awards awarded by the Department of Defense on or before Dec 19, 2017 that will be performed in the United States Central Command (USCENTCOM) theater of

operations.

(b) The substance of this clause, including this paragraph (b), is required to be included in subawards or contracts under this grant or cooperative agreement that have an estimated value over \$50,000 and will be performed outside the United States, including its outlying areas.

(End of term)

Section B. Additional requirements.

☒ 1. Prohibition on Using Funds under Grants and Cooperative Agreements with Entities that Require Certain Internal Confidentiality Agreements.

a. You may not require your employees, contractors, or subrecipients seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting them from lawfully reporting that waste, fraud, or abuse to a designated investigative or law enforcement representative of a federal department or agency authorized to receive such information.

b. You must notify your employees, contractors, and subrecipients that the prohibitions and restrictions of any internal confidentiality agreements inconsistent with paragraph a. of this award provision are no longer in effect.

c. The prohibition in paragraph 1.a. of this section does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

d. If the Federal Government determines that you are not in compliance with this award provision, it:

i. Will prohibit your use of funds under this award, in accordance with section 743 of Division E of the Consolidated and Further Continuing Resolution Appropriations Act, 2015, (Public Law 113-235) or any successor provision of law; and

ii. May pursue other remedies available for your material failure to comply with award terms and conditions

AFRL AWARD-SPECIFIC TS&CS TO DOD R&D GENERAL TERMS AND CONDITIONS

The following Ts&Cs with checked blocks are hereby incorporated into your award:

FMS -- AWARD-SPECIFIC TERMS AND CONDITIONS

☒ 1. Incremental Funding (Feb 2024)

a. Allotted and Currently Available for Payment. The Government's share for full performance of this award is shown in Block 20.C. of the Award Form under Federal Share. Of this amount, only that shown in Block 20.B. of the Award Form under Federal Share is allotted and currently available for payment. In no event is the Government obligated to reimburse you for expenditures in excess of the total funds allotted by the Government. We anticipate that from time-to-time additional amounts will be allotted to this agreement by unilateral modification until the total Government share is fully funded.

b. Recipient Notification to Government. You shall notify the AFRL GO in writing whenever expenditures, including anticipated expenditures over the next 60 days, are expected to exceed 75% of the amount allotted (including your cost share, if applicable).

c. Agreement of Parties. The parties agree that if additional funds are not allotted, this agreement may be terminated. You are not obligated to continue performance or otherwise incur costs in excess of the amount then allotted by the Government to the agreement plus your corresponding share, until the AFRL GO notifies you in writing that the amount allotted by the Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to this agreement. When and to the extent that the amount allotted by the Government to the agreement is increased, any costs you incur before the increase that are in excess of the amount previously allotted by the Government to the agreement plus your corresponding share, shall be allowable to the same extent as if incurred afterward, unless the AFRL GO issues a termination or other notice and directs that the increase is solely to cover termination or other specified expenses. Planned funding periods and amounts are shown in the Incremental Funding Periods section of the grant. If options are listed in the funding table, options are not guaranteed and may only be exercised in writing by the AFRL GO.

☐ 2. Cost Sharing Summary Schedule (Feb 2024)

a. The parties estimate that the research and development work under this award can only be accomplished with the recipient aggregate resource contribution shown in Block 20.C. of Award Form under Non-Federal Share throughout the term of the award. The recipient agrees to provide these resources as shown below. Failure of either party to provide its respective total contribution may result in a unilateral amendment to the award by the AFRL GO to reflect a proportional reduction in funding for the other party.

b. The recipient's contributions may count as cost sharing only to the extent that they comply with the criteria at 2 CFR 1128.610.

c. The recipient agrees to cost share in proportion to the Incremental Funding Periods section of this grant. This schedule may be amended annually to reflect changes or updates resulting from the annual program planning process.

☒ 3. Allotted Funding (Feb 2024)

The following funds are allotted to this agreement: See Block 20 of the Award Form.

Payment Instructions for Multiple Accounting Classification Citations: See FMS Article II, Section C, Paragraph d.

☒ 4. Scope and Management of the Program (Feb 2024)

Duty of Good Faith. We, the Government and you, the recipient, are bound to each other by a duty of good faith and best effort to achieve the goals of this agreement. This agreement is not intended to be, nor shall it be construed as, by implication or otherwise, a partnership, a corporation, or other business organization.

Research and Development Program. You shall perform a coordinated research and development program carried out in accordance with the Grantee's Proposal as stated in Block 19 of the Award Form. The recipient shall submit all documentation required by the DoD R&D General Ts&Cs Part 5, REP Article(s) I - IV, Financial, Programmatic, and Property Reporting and AFRL Addendum guidance contained herein for each individual award.

Coordinated Research Program. You, the recipient, shall accomplish the overall management, including technical, programmatic, reporting, and financial and administrative matters of the coordinated research program established under each individual award. The Government Technical Representative / Program Office(s) may interact with the recipient to promote effective collaboration between the recipient and the Government.

☒ 5. Food and Beverage (Feb 2024)

Food and Beverage. Funds may not be used to pay for food or beverages (unless preapproved by the AFRL GO). Funds may never be used to pay for alcoholic beverages, even if food and beverages are approved by the AFRL GO.

PROP – AWARD-SPECIFIC Ts&Cs

☐ 6. Base Support (Feb 2024).

Base support may be provided by the Government to the Recipient as follows.

The Recipient will require use of base support on a rent-free, non-interference basis to include Government-controlled working space, material, equipment, services (including automatic data processing), or other support (excluding use of the Defense Switched Network (DSN)) which the Government determines can be made available at, or through, any Air Force installation where this agreement shall be performed.

Unless otherwise stipulated in the award schedule, the Recipient will use base support on a no-charge-for-use basis and the value shall be a part of the Government's agreement consideration.

The Recipient will immediately report (with a copy to the AGO) inadequacies, defective base support, or nonavailability of support stipulated by the award schedule, together with a recommended plan for

obtaining the required support. Facilities are not to be purchased under this agreement by the Recipient. Additionally, the Recipient (or authorized representative) will not purchase or otherwise furnish any base support requirement provided by the SOW (or authorize others to do so), without prior written approval of the AFRL GO regarding the price, terms, and conditions of the proposed purchase, or approval of other arrangements.

The base support to be furnished under this award is N/A. Because of the nature and location(s) of the work performed, the value of such support is undeterminable. The Recipient is not authorized to incur any costs resulting from nonsupport prior to AFRL GO direction.

In the performance of this agreement or any major subawards, no direct or indirect costs for support will be incurred if the Government determines that support is available at or through any Air Force installation where this agreement shall be performed.

Written authorization must be requested from the AFRL GO for support not later than 90 days before the required in-place dates at each Air Force installation, and immediately for any required changes. Ensure the facilities are available and concurrence for their use has been obtained from the cognizant AFRL GO before finalizing award negotiations and/or source selection. In competitive environments, the request for proposal/request for quote (RFP/Rfq) should request the Offeror propose a cost in the event that the facilities are not available. This is necessary in order to make a valid comparison of all Offerors' proposals.

[] 7. Federally Owned Property (Feb 2024)

- a. The Government will provide the following Federally owned property to the Recipient
- b. Title to any federally owned property that the Government provides to the recipient under this award (or for which accountability is transferred to this award from another Federal award) remains with the Federal Government.
- c. Refer to the DoD R&D Ts&Cs, Part 2, Property Administration, for details on Federally Owned Property pertaining to title, property management systems, and use and disposition instructions.

[X] 8. Access to USAF Bases, AFRL Facilities and/or US Government Information Technology Networks – Information Regarding Non-US Citizens Assigned to this Project (Feb 2024)

1. Information Regarding Non-US Citizens Assigned to this Project:

a. Any of your employees requiring access to USAF bases, AFRL facilities, and/or access to US Government Information Technology networks in connection with the work on this agreement must be US citizens. Possession of a permanent resident card ("Green Card") does not equate to US citizenship. This requirement does not apply to foreign nationals approved by the US Department of Defense or US State Department under international personnel exchange agreements with foreign governments. Any waivers to this requirement must be granted in writing by the AFRL GO prior to providing access. The above requirements are in addition to any other agreement requirements related to obtaining a Common Access Card (CAC).

b. For purposes of paragraph a above, if an IT network/system does not require AFRL to endorse a Recipient's application to said network/system in order to gain access, the organization operating the IT network/system is responsible for controlling access to its system. If an IT network/system requires a U.S. Government sponsor to endorse the application in order for access to the IT network/system, AFRL will only endorse the following types of applications, consistent with the requirements above:

- i. Recipient employees who are U.S. citizens performing work under this award.

- ii. Recipient employees who are non-U.S. citizens and who have been granted a waiver.
- iii. Any additional access restrictions established by the IT network/system owner apply.

[] 9. Recipient Access to Air Force Installations (Feb 2025).

- a. Identification and Passes. You must obtain base identification and vehicle passes, if required, for all recipient personnel who make frequent visits to or perform work on the Air Force installation(s) cited in this agreement. Your personnel are required to wear or prominently display installation identification badges or recipient-furnished, recipient identification badges while visiting or performing work on the installation.
- b. Written Requests. You must submit a written request on company letterhead to the Government Technical Representative / Program Office listing the following: award number, location of work site, start and stop dates, and names of employees and subcontractor/subrecipient employees needing access to the base. The letter will also specify the individual(s) authorized to sign for a request for base identification credentials or vehicle passes. The Government Technical Representative / Program Office will endorse the request and forward it to the issuing base pass and registration office or Security Forces for processing. When reporting to the registration office, your authorized personnel/individual(s) should provide a valid driver's license, current vehicle registration, valid vehicle insurance certificate, and comply with local security procedures to obtain a vehicle pass. Please contact the Government Technical Representative / Program Office to request applicable local security procedures.
- c. New Personnel. During performance of the award, you are responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials and vehicle passes for any employee or sub-contractor or sub-recipient who no longer requires access to the work site.
- d. Unescorted Entry to Controlled or Restricted Areas. When work under this award requires unescorted entry to controlled or restricted areas, you must comply with local security procedures as applicable. Please contact the Government Technical Representative / Program Office to request applicable local security procedures.
- e. Actions Upon Completion or Termination of Agreement. Upon completion or termination of this agreement or expiration of the identification passes, you must ensure that all base identification passes issued to employees and subcontractor/subrecipient employees are returned to the issuing office.

[] 10. Common Access Cards (CACs) for Recipient Personnel (Feb 2024)

- 1. For installation(s)/location(s) cited in the award, you shall ensure Common Access Cards (CACs) are obtained by all awardee or subcontract/subrecipient personnel who meet one or both of the following criteria:
 - a. Require logical access to Department of Defense computer networks and systems in either:
 - i. the unclassified environment; or
 - ii. the classified environment where authorized by governing security directives.

b. Perform work which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

2. You and your personnel shall use the following procedures to obtain CACs:

a. You must provide a listing of personnel who require a CAC to the AFRL GO. The government will provide the recipient instruction on how to complete the Contractor Verification System (CVS) application and then notify the recipient when approved.

b. Your personnel shall obtain a CAC from the nearest Real Time Automated Personnel Identification Documentation System (RAPIDS) Issuing Facility (typically the local Military Personnel Flight (MPF)).

3. While visiting or performing work on installation(s)/location(s), your personnel (and sub-recipient and sub-contractor personnel) must wear or prominently display the CAC as required by the governing local policy.

4. During the performance period of the award, you must:

a. Within 7 working days of any changes to the listing of your personnel authorized a CAC, provide an updated listing to the AFRL GO who will provide the updated listing to the authorizing government official;

b. Return CACs in accordance with local policy/directives within 7 working days of a change in status for your personnel who no longer require logical or physical access;

c. Return CACs in accordance with local policy/directives within 7 working days following a CACs expiration date; and

d. Report lost or stolen CACs in accordance with local policy/directives.

5. Within 7 working days following completion/termination of the award, you must return all CACs issued to their personnel to the issuing office or the location specified by local policy/directives.

6. Failure to comply with these requirements may result in withholding of final payment.

[] 11. Local Guidance, Health and Safety on Government Installations (Feb 2024)

1. Work on Government Installation. In performing work under this Agreement on a Government installation, the recipient shall:

a. Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of recipient and Government personnel performing or in any way coming in contact with the performance of this award; and

b. Take such additional immediate precautions as the AFRL GO may reasonably require for health and safety purposes.

i. The AFRL GO may, by written order, direct Air Force Occupational Safety and Health (AFOSH) Standards and/or health/safety standards as may be required in the performance of this Agreement and any

adjustments resulting from such direction will be in accordance with the modifications article of this award.

ii. Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the AFRL GO, shall be grounds for termination of this Agreement in accordance with the Termination article of this award.

[X] 12. Subject Inventions (Feb 2024). DoD adopts the Governmentwide patent rights award clause at 37 CFR 401.14 as described in the DoD R&D General T&Cs PROP Article VI. 37 CFR 401.14(l) requires designation of a central point of contact for communication matters relating to the clause. AFRL designates the servicing Staff Judge Advocate Office.

a. Subject Inventions (Patent) Report. Interim Invention Information shall be included as a required part of the Interim Performance Report.

b. Submit a Final Invention Report in accordance with the DoD R&D General T&Cs PROP Article VI and the Reporting Information section of the grant. Intangible Property, Section B. The DD Form 882, "Report of Inventions and Subcontracts" shall be used to submit these reports. The report must: (1) list all subject invention(s) and state that all subject inventions have been disclosed, or (2) state that there are no such inventions. The report must be filed at the end of the term for this award and is due 90 days after the expiration of the final performance period as shown in the Reporting Information section of the grant. Negative reports are also required.

c. Distribution. See the Reporting Information section of the grant.

d. Subcontract or Subaward Reporting. The DD Form 882 shall be used for the notification of any subaward(s) for experimental, developmental or research work which contains a "Patent Rights" clause, with a cc: to the Government Technical Representative / Program Office.

e. Other Notifications. All other notifications required by the award shall also be sent to the individuals in para. b. above.

f. Retained Ownership: For subject inventions for which the awardee has or will retain ownership, the following information must be submitted to those listed in para. b. above: 1) the filing date, 2) the serial number and title, 3) the name(s) of inventor(s), 4) a copy of the patent application and 5) the patent number and issue date.

OAR – AWARD-SPECIFIC Ts&Cs

[X] 13. Administrative Responsibilities (Feb 2024)

Questions regarding administrative, technical and intellectual matters should be referred to the personnel identified for each matter herein.

The Government representatives for your award are:

AFRL Awarding Office:
See the Award Form

AFRL Government Technical Representative (Project Manager) or Program Officer: See the Award Form or the Address Information section

Field Administration Office: See the Award Form and/or the Address Information section

The Recipient representatives for your award are:

Recipient Administrator/Business Office POC:
See the Award Form and/or the Address Information section

Recipient Principal Investigator (PI):
See the Award Form and/or the Address Information section

[X] 14. Delegation of Administration (Feb 2024)

The administrative duties listed below have been delegated to the field administration office:

1. During performance:

a. Perform property administration.

b. Perform plant clearance.

c. Perform cash management by reviewing quarterly Federal Financial Report (SF 425) and, after conferring with the AFRL GO, make appropriate adjustments to predetermined scheduled payments by modifying the agreement.

2. Upon expiration of agreements:

a. Obtain the final Federal Financial Report (SF 425).

b. Obtain final property report and dispose of Government property on those assistance awards containing residual Government Property.

c. Perform a review of final incurred costs and assist the AFRL GO in resolving exceptions, if any, resulting from questioned costs.

d. Perform cost sharing adjustments, if applicable.

e. Assure that all refunds due the Government are received.

f. Notify the AFRL GO when the final SF270 and/or SF425 indicates an unexpended balance.

[X] 15. Ombudsman (May 2025)

a. An Ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and others for this agreement. When requested, the Ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the Ombudsman does not affect the authority of the Government Technical Representative / Program Office, AFRL GO, or evaluation officials. Further, the Ombudsman does not participate in the evaluation of proposals, the evaluation

process, or the adjudication of protests or formal grant/cooperative agreement disputes. The Ombudsman may refer the party to another official who can resolve the concern.

b. Before consulting with the Ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the AFRL GO for resolution. Consulting the Ombudsman does not alter or postpone the timelines for any other processes.

c. If a resolution cannot be made by the AFRL GO, concerned parties may contact the AFRL Ombudsman, AFRL/PK Technical Director, HQ AFRL/PK. The AFRL Alternate Ombudsman is the Deputy Director of Contracting, HQ AFRL/PK. Please send an email to afrl.pk.workflow@us.af.mil with the subject of "Ombudsman."

d. The Ombudsman has no authority to render a decision that binds the agency.

e. Do not contact the Ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries must be directed to the AFRL GO.

[X] 16. Modifications (Feb 2024)

a. Modifications to this agreement may be proposed by either party. Your recommendations for any modifications to this agreement shall be submitted in writing to the AFRL GO/Awarding Office before the desired effective date with a copy to the Government Technical Representative / Program Office. You must detail the technical, chronological, and financial impact of the proposed modification to the program. Changes are effective only after the agreement has been modified. ONLY an AFRL GO has the authority to act on behalf of the Government to modify this agreement. If the Government agrees to the proposed modification without change, an AFRL GO may issue a modification unilaterally approving the request.

b. The AFRL GO or AGO may unilaterally issue minor or administrative agreement modifications (e.g., changes in the paying office or appropriation data, changes to Government personnel identified in the agreement, etc.).

[X] 17. Extending the Term (Feb 2024). If the parties agree, the term of this agreement may be extended if funds are available and research opportunities reasonably warrant. Any extension shall be formalized through modification of the agreement by the AFRL GO and you, the awardee.

[X] 18. Termination (Feb 2024). If you initiate a partial or full termination in accordance with DoD General Research T&Cs OAR Article III.C.1.c, you must provide the AFRL GO and AGO the required written notification at least 30 days prior to the effective date of the termination.

[X] 19. Controlled Unclassified Information (Feb 2024). The parties understand that information and materials provided pursuant to or resulting from this award may be export controlled, sensitive, for official use only or otherwise protected by law, executive order or regulation. The recipient is responsible for compliance with all applicable laws and regulations. Nothing in this award shall be construed to permit any disclosure in violation of those restrictions.

[X] 20. Reporting Potentially Classifiable Information (Feb 2024). You must immediately notify the Government Technical Representative / Program Office if you identify any potentially classifiable information under this award.

[X] 21. Export Control (Feb 2024)

1. Definition. "Export-controlled items," as used in this article, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes:

a. "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120.

b. "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.

2. The Recipient shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for awardees to register with the Department of State in accordance with the ITAR. The Recipient shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.

3. The Recipient's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this article.

4. Nothing in the terms of this award adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to—

a. The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.);

b. The Arms Export Control Act (22 U.S.C. 2751, et seq.);

c. The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);

d. The Export Administration Regulations (15 CFR Parts 730-774);

e. The International Traffic in Arms Regulations (22 CFR Parts 120-130); and

f. Executive Order 13222, as extended.

5. The Recipient shall include the substance of this article, including this paragraph (e), in all subawards.

6. Access to the technology developed under this agreement by foreign firms, institutions or individuals shall be controlled by the recipient under applicable U.S. export control laws.

7. The recipient shall receive the AFRL GO's approval before assigning or granting access to any work, equipment, or technical data generated or delivered under this agreement, other than public domain, to

foreign persons or their representatives. The notification shall include the name and country of origin of the foreign person or representative, the specific work, equipment, or data to which the person will have access.

[X] 22. Disclosure of Information (Feb 2024)

1. Disclosure of Information: You must not release to anyone outside your organization any unclassified information, regardless of medium (e.g., film, tape, document, media announcements, etc.), pertaining to any part of this agreement or any program related to this agreement unless-

a. The AFRL GO has given prior written approval;

b. The information is otherwise in the public domain before the date of release; or

c. The information results from or arises during the performance of a project that has been scoped and negotiated by the awarding office with you, the non-Federal entity and research performer, and determined in writing by the Grants or Agreements Officer to be fundamental research in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of award and the USD (AT&L) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008.

2. Approval Requests: Your requests for approval under paragraph 1.c. must identify the specific information to be released, the medium to be used, and the purpose for the release. You must submit your request to the AFRL GO at least 65 days before the proposed date for release.

3. Subaward/Subcontract: You agree to include a similar requirement in each sub-agreement under this agreement. Subawardees must submit requests for authorization to release information through you to the AFRL GO.

[X] 23. Fundamental Research (Feb 2024) Pursuant to the Disclosure of Information Article, the exception in paragraph 1.c., allowing release of information is applicable to Grantee's proposal as stated in Block 19 of the Award Form, only as long as the work remains in the public domain or is considered fundamental research and not sensitive or inappropriate for public release. Any time work progresses to the non-public domain, exceeds the scope of fundamental research, or the Recipient has reason to believe the work has become sensitive or inappropriate for release to the public, then this exception no longer applies.

[] 24. Using Classified Data (Feb 2024)

a. It is anticipated that you will require access to, or generate, classified data. You must comply with the attached Security Classification Specification (DD Form 254).

[X] 25. Using Technical Information Resources (Feb 2024). To the extent practical, you must use the technical information resources of the Defense Technical Information Center (DTIC) and other Government or private facilities to investigate recent and on-going research and avoid needless

duplication of scientific and engineering effort.

☒ 26. Publishing Project Results (Feb 2024)

a. Publications. Publication of results of the research project in appropriate professional journals is encouraged as an important method of recording and reporting scientific information. One copy of each paper planned for publication will be submitted to the Government Technical Representative / Program Office (identified in Administrative Responsibilities Article) simultaneously with its submission for publication. Following publication, copies of published papers shall be submitted to the Government Technical Representative / Program Office.

b. Disclaimer and Acknowledgement. You agree that when releasing information relating to this award, the release shall include a statement to the effect that the project or effort undertaken was or is sponsored by the Department of the Air Force, AFRL. You are responsible for assuring that every publication of material (including World Wide Web pages) based on or developed under this award, except scientific articles or papers appearing in professional journals, contains the following disclaimer:

"The opinions, findings, views, conclusions or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the DAF, AFRL or the U.S. Government."

You are responsible for including an acknowledgment of the awarding agency's support, which shall appear in the publication of any material, whether copyrighted or not. The acknowledgement must read:

"This material is based on research sponsored by the Air Force Office of Scientific Research under agreement number [recipient enter award number from Block 1 of the Award Form]. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon."

c. Distribution Statement. You are responsible for assuring that every publication of material based on or developed under this project contains the distribution statement stated in REP Article I, Section A, paragraph 3.

d. Compliance. Nothing in the foregoing shall affect your responsibility to comply with the requirements contained in the DoD R&D General Ts&Cs and in these AFRL Award Specific Ts&Cs, such as the requirement for you to include measures to safeguard any information that Federal statute, Executive order, or regulation requires to be protected (e.g., controlled unclassified information, personally identifiable information or export controlled information) to include information generated under the award or provided to you and identified as being subject to protection.

e. Copyright. Any transfer of copyright ownership in a publication will provide that the transfer of copyright ownership is subject to the United States Government's royalty-free license throughout the world in all copyrightable material contained in the publications including, but is not limited to, news releases, articles, manuscripts, brochures, advertisements, still and motion pictures, speeches, trade association proceedings, and symposia.

☐ 27. Activities Abroad (Feb 2024). You must ensure that project activities carried on outside the United States are coordinated as necessary with appropriate Government authorities and that appropriate licenses, permits, or approvals are obtained prior to undertaking proposed activities. The awarding agency does not assume responsibility for awardee compliance with the laws and regulations of the

country in which the activities are to be conducted.

[] 28. Air Force Research Laboratory Wright Research Site Security Requirements (SEP 2023)
Definitions. As used in this article –

Air Force Research Laboratory (AFRL)-managed facilities means -

AFRL buildings, areas, test facilities, and laboratories located at the AFRL Wright Research Site, Wright-Patterson Air Force Base (WPAFB), Ohio; Buildings owned or facility space leased by the AFRL Wright Research Site, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of the AFRL Wright Research Site;

Commercial space managed by the AFRL Wright Research Site that is shared with non-government tenants. For example, if the AFRL Wright Research Site leased the 10th floor of a commercial building, the directive applies to the 10th floor only; Awardee-operated facilities owned by the AFRL Wright Research Site, including laboratories engaged in national defense research and production activities.

Augmented reality (AR) device means a device that is capable of, or assists in, augmented reality by enhancing or creating digital overlays. AR is used to enhance natural environments or situations and offers perceptually enriched and interactive experiences achieved through digital visual elements, sounds, and other sensory stimuli via holographic technology. Examples include, but are not limited to, hardware components such as display sensors, computers, projectors, input devices, mobile devices, eyewear, wireless communication devices, and cameras.

Data storage device means computer hardware used to remember/store data. Examples include, but are not limited to, remote or autonomous drones, CDs, DVDs, Blue-Rays, USB flash drives, jump/stick/pen drives, external hard drives, solid state drives, cloud storage, mainframes, laptops, desktops, and floppy disks.

Formal investigation means the process of investigation ordered by a competent U.S. Government authority that involves the questioning of involved parties and gathering of data with the intent to determine if classified or controlled unclassified information (CUI) was lost, compromised, suspected to be compromised, or not compromised at all.

Personal means items that are owned by an individual, person, or private entity and not provided for use under this grant or agreement by the U.S. Government.

Physical computer network means interconnected computing devices of any kind that can exchange data and share resources or communicate with other types of devices to execute operations or store information of any kind.

Security Incident Investigation (SII) means a formal investigation that occurs when there is a known or suspected loss of national security information (NSI) or CUI. U.S. Government security personnel conduct SII to (1) determine the circumstances surrounding an actual or potential compromise of NSI or CUI; (2) ascertain individual responsibility; (3) notify outside stakeholders, when necessary; and (4) make recommendations to prevent similar occurrences in the future.

Virtual device means a device with no associated hardware. A virtual device mimics a physical hardware device when, in fact, it exists only in software form. Therefore, the device makes the system believe that a particular hardware exists when in reality it does not. Examples include, but are not limited to, a computer, tablet, or smartphone that is simulated in a computer.

Prohibition. The following is prohibited within AFRL-managed facilities, except when explicitly authorized by a U.S. Government grant or agreement:

Prohibited activities - Photography Videography Live Streaming Recordings of any kind (e.g., audio)
Prohibited personal networks and devices - AR devices Virtual devices Wi-Fi networks Physical computer networks Data storage devices

Waivers. A request for a waiver to the prohibitions outlined in paragraph (b) shall be submitted in writing to the Government Technical Representative / Program Office for internal Government coordination and approval. If a waiver request is granted, written approval shall be provided by the cognizant AFRL Operations Security (OPSEC) coordinator and Security Chief. The specific format for a waiver request will be provided upon request to the Government Technical Representative / Program Office.

Incident Reporting Requirement. If the awardee discovers a prohibited activity identified in paragraph (b)(1) has occurred within an AFRL-managed facility and/or a prohibited personal network or device identified in paragraph (b)(2) has been brought into an AFRL-managed facility without a valid waiver, as specified in paragraph (c), the incident shall be immediately reported in writing to the Government Technical Representative / Program Office with a courtesy copy to the Grant/Agreement Officer.

Violations. If a violation of this article occurs or is suspected to have occurred, the cognizant AFRL security organization will lead and conduct a formal investigation. If a violation or suspected violation may involve classified material, the cognizant AFRL security organization will lead and conduct a Security Incident Investigation (SII). Depending on the outcome of the investigation and the information involved, penalties for violations can range from a written warning to removal from the AFRL-managed facility and/or installation. Violations and potential penalties will be governed by the applicable articles(s), law(s), or regulation(s).

Subawards/Subcontracts. The awardee shall include this article in all subawards/subcontracts or similar contractual instruments/agreements relating to work performed under this grant or agreement.

[X] 29. Science and Technology (S&T) Protection (Feb 2024). The requirements below are in accordance with Air Force Research Laboratory Instruction (AFRLI) 61-113, "Science and Technology (S&T) Protection for the Air Force Research Laboratory."

Initial/Annual/New SF 424, Research and Related Senior/Key Person Profile (Expanded) Form,
Requirement: The awardee shall provide a SF 424 with the following information:

Initial SF 424: An initial report of all Senior/Key Personnel at the time of award. This form is required with proposal submission.

Annual SF 424: An annual report of all Senior/Key Personnel providing support. The first submission is due within 30 days after 12 months after receipt of award. Subsequent submissions are due every 12 months after first annual submission, and throughout the technical effort.

New/Revised SF424: A new or revised SF 424 report must be made whenever any new Senior/Key Personnel participate on the contract, agreement, grant, or OT. Any updated SF 424s for new Senior/Key Personnel supporting the award require coordination from the Government prior to the awardee employee receiving access to S&T information. These reports are required to provide updates and

supplements to the SF 424 as appropriate during the period of performance. Identify changes from previous versions. Permanent change pages shall conform to the requirements, quality, style, and format of the basic documentation.

Submission: Annual and Revised SF 424s shall be submitted electronically in Microsoft Office Suite compatible format, PDF, or RTF as coordinated with the Government Technical Representative / Program Office. For email delivery, include the award number in the subject line. The recipient shall submit one copy of the SF 424 to:

AFRL Program Officer (See the Award Form or the Address Information section)
AFRL/IP Security (afosr.ip@us.af.mil)

Note: Submit classified Data (up to and including SECRET) via the SIPRNET or as coordinated with the requiring office. Submit Export Controlled Data as coordinated with the requiring office.

Note: Submit electronically. Electronic submittals shall be encrypted or password protected. Mark all data delivered with the following Distribution Statement: Distribution authorized to U.S. Government Agencies and their contractors.

[X] 30. Prohibition on a ByteDance Covered Application (Jun 2023)

Definitions. As used in this article—

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited. Information technology, as defined in 40 U.S.C. 11101(6)—

a. Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by an awardee under an award with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

b. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal awardee incidental to a Federal award.

2. Prohibition. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, “No TikTok on Government Devices” Implementation Guidance, collectively prohibit the presence or use of a covered application on

executive agency information technology, including certain equipment used by Federal awardee(s). The Awardee is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Awardee under this award, including equipment provided by the Awardee's employees; however, this prohibition does not apply if the Grants Office/Agreements Officer provides written notification to the Awardee that an exception has been granted in accordance with OMB Memorandum M-23-13.

3. Subcontracts/Subrecipients. The Awardee shall insert the substance of this article, including this paragraph (c), in all subawards, including subawards for the acquisition of commercial products or commercial services.

[X] 31. Safeguarding Covered Defense Information and Cyber Incident Reporting (May 2024)

(a) Definitions. As used in this article—

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Recipient attributional/proprietary information” means information that identifies the recipient(s), whether directly or indirectly, by the grouping of information that can be traced back to the recipient(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered recipient information system” means an unclassified information system that is owned, or operated by or for, a recipient and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the award and provided to the recipient by or on behalf of DoD in support of the performance of the award; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the recipient in support of the performance of the award.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered recipient information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

“Computer software” means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.

“Technical data” means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data financial, administrative, cost or pricing, or management information, or information incidental to award administration.

(b) Adequate security. The Recipient shall provide adequate security on all covered recipient information systems. To provide adequate security, the Recipient shall implement, at a minimum, the following information security protections:

(1) For covered recipient information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the article , Cloud

Computing Services, of this award.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this award.

(2) For covered recipient information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this article, the covered recipient information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" Revision 2 (available via the internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>) in effect at the time the solicitation is issued or as authorized by the Grants/Agreements Officer.

(ii)(A) The Recipient shall implement NIST SP 800-171. The Recipient shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of award, of any security requirements specified by NIST SP 800-171 not implemented at the time of award.

(B) The Recipient shall submit requests to vary from NIST SP 800-171 in writing to the Grants/Agreements Officer, for consideration by the DoD CIO. The Recipient need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the recipient's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Grants/Agreements Officer when requesting its recognition under this award.

(D) If the Recipient intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this award, the Recipient shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/resources/documents/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this article for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Recipient reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this article, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Recipient discovers a cyber incident that affects a covered recipient information system or the covered defense information residing therein, or that affects the recipient's ability to perform the requirements of the award that are designated as operationally critical support and identified in the award, the Recipient shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered recipient information system(s) that were part of the cyber incident, as well as other information systems on the Recipient's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Recipient's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <https://dibnet.dod.mil>.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <https://dibnet.dod.mil>.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this article, the Recipient or subrecipient/subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <https://public.cyber.mil/eca/>.

(d) Malicious software. When the Recipient or subrecipient(s)/subcontractor(s) discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Grants/Agreements Officer. Do not send the malicious software to the Grants/Agreements Officer.

(e) Media preservation and protection. When a Recipient discovers a cyber incident has occurred, the Recipient shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this article and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Recipient shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Grants/Agreements Officer will request that the Recipient provide all of the damage assessment information gathered in accordance with paragraph (e) of this article.

(h) DoD safeguarding and use of recipient attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the recipient (or derived from information obtained from the recipient) under this article that includes recipient attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Recipient shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the recipient attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of recipient attributional/proprietary information not created by or for DoD. Information that is obtained from the recipient (or derived from information obtained from the recipient) under this article that is not created by or for DoD is authorized to be released outside of DoD.

- (1) To entities with missions that may be affected by such information;
 - (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
 - (3) To Government entities that conduct counterintelligence or law enforcement investigations;
 - (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
 - (5) To a support services contractor ("recipient") that is directly supporting Government activities under an award that includes the article, Limitations on the Use or Disclosure of Third-Party Recipient Reported Cyber Incident Information.
- (j) Use and release of recipient attributional/proprietary information created by or for DoD. Information that is obtained from the recipient (or derived from information obtained from the recipient) under this article that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this article) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this article, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.
- (k) The Recipient shall conduct activities under this article in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.
- (l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this article in no way abrogates the Recipient's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable articles of this award, or as a result of other applicable U.S. Government statutory or regulatory requirements.
- (m) Subawards/Subcontracts. The Recipient shall—
- (1) Include this article, including this paragraph (m), in subawards/subcontracts, or similar contractual instruments, for operationally critical support, or for which subaward/subcontract performance will involve covered defense information, including subaward/subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Recipient shall determine if the information required for subaward/subcontractor performance retains its identity as covered defense information and will require protection under this article, and, if necessary, consult with the Grants/Agreements Officer; and
 - (2) Require subawards/subcontractors to—
 - (i) Notify the prime Recipient (or next higher-tier subaward/subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Grants/Agreements Officer, in accordance with paragraph (b)(2)(ii)(B) of this article; and
 - (ii) Provide the incident report number, automatically assigned by DoD, to the prime Recipient (or next higher-tier subaward/subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this article.

[] 32. Limitations on the Use or Disclosure of Third-Party Recipient Reported Cyber Incident Information (Feb 2024)

(a) Definitions. As used in this article—

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered defense information” means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the award or order and provided to the recipient by or on behalf of DoD in support of the performance of the award; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the recipient in support of the performance of the award.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered recipient information system.

“Technical information” means technical data or computer software. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

“Computer software” means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer

data bases or computer software documentation.

“Technical data” means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data financial, administrative, cost or pricing, or management information, or information incidental to award administration.

(b) Restrictions. The Recipient agrees that the following conditions apply to any information it receives or creates in the performance of this award that is information obtained from a third-party’s reporting of a cyber incident pursuant, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that article):

(1) The Recipient shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government’s activities related to article, Safeguarding Covered Defense Information and Cyber Incident Reporting, and shall not be used for any other purpose.

(2) The Recipient shall protect the information against unauthorized release or disclosure.

(3) The Recipient shall ensure that its employees are subject to use and non-disclosure obligations consistent with this article prior to the employees being provided access to or use of the information.

(4) The third-party recipient that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Recipient, as required by paragraph (b)(3) of this article.

(5) A breach of these obligations or restrictions may subject the Recipient to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this article.

(c) Subawards/Subcontracts. The Recipient shall include this article, including this paragraph (c), in subawards/subcontracts, or similar contractual instruments, for services that include support for the Government’s activities related to safeguarding covered defense information and cyber incident reporting, including subawards/subcontracts for commercial items, without alteration, except to identify the parties.

[] 33. Cloud Computing Services (Feb 2024)

(a) Definitions. As used in this article—

“Authorizing official,” as described in DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

“Cloud computing” means a model for enabling ubiquitous, convenient, on-demand network access to a

shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Government data” means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

“Government-related data” means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a recipient through the storage, processing, or communication of Government data. This does not include recipient’s business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Media” means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

“Spillage” security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

(b) Cloud computing security requirements. The requirements of this article are applicable when using cloud computing to provide information technology services in the performance of the award.

(1) If the Recipient indicated in its offer that it “does not anticipate the use of cloud computing services in the performance of a resultant award,” in response to provision, Representation of Use of Cloud Computing, and after the award of this award, the Recipient proposes to use cloud computing services in the performance of the award, the Recipient shall obtain approval from the Grant/Agreement Officer prior to utilizing cloud computing services in performance of the award.

(2) The Recipient shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Grants/Agreements Officer) found at <https://public.cyber.mil/dccs/dccs-documents/> unless notified by the Grant/Agreement Officer that this requirement has been waived by the DoD Chief Information Officer.

(3) The Recipient shall maintain within the United States or outlying areas all Government data that is not physically located on DoD premises, unless the Recipient receives written notification from the Grant/Agreement Officer to use another location.

(c) Limitations on access to, and use and disclosure of Government data and Government-related data.

(1) The Recipient shall not access, use, or disclose Government data unless specifically authorized by the terms of this article or an order issued hereunder.

(i) If authorized by the terms of this award or an order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this award or order.

(ii) The Recipient shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this award.

(2) The Recipient shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Grant/Agreement Officer.

(d) Cloud computing services cyber incident reporting. The Recipient shall report all cyber incidents that are related to the cloud computing service provided under this award. Reports shall be submitted to DoD via <http://dibnet.dod.mil/>.

(e) Malicious software. The Recipient or subaward/subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Grant/Agreement Officer.

(f) Media preservation and protection. When a Recipient discovers a cyber incident has occurred, the Recipient shall preserve and protect images of all known affected information systems identified in the cyber incident report (see paragraph (d) of this article) and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(g) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Recipient shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(h) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Grant/Agreement Officer will request that the Recipient provide all of the damage assessment information gathered in accordance with paragraph (f) of this article.

(i) Records management and facility access.

(1) The Recipient shall provide the Grant/Agreement Officer all Government data and Government-related data in the format specified in the award.

(2) The Recipient shall dispose of Government data and Government-related data in accordance with the

terms of the award and provide the confirmation of disposition to the Grant/Agreement Officer in accordance with award closeout procedures.

(3) The Recipient shall provide the Government, or its authorized representatives, access to all Government data and Government-related data, access to recipient personnel involved in performance of the award, and physical access to any Recipient facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

(j) Notification of third party access requests. The Recipient shall notify the Grant/Agreement Officer promptly of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Recipient shall cooperate with the Grant/Agreement Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.

(k) Spillage. Upon notification by the Government of a spillage, or upon the Recipient's discovery of a spillage, the Recipient shall cooperate with the Grant/Agreement Officer to address the spillage in compliance with agency procedures.

(l) Subawards/Subcontracts. The Recipient shall include this article, including this paragraph (l), in all subawards/subcontracts that involve or may involve cloud services, including subawards/subcontracts for commercial services.

[X] 34. NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (Feb 2024)

(a) Definitions.

“Basic Assessment” means a recipient's self-assessment of the recipient's implementation of NIST SP 800-171 that—

(1) Is based on the Recipient's review of their system security plan(s) associated with covered recipient information system(s);

(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and

(3) Results in a confidence level of “Low” in the resulting score, because it is a self-generated score. “Covered recipient information system” has the meaning given in the article, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this award.

“High Assessment” means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a recipient's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Recipient's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the recipient's system

security plan; and

(iv) Discussions with the recipient to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of “High” in the resulting score.

“Medium Assessment” means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a recipient’s Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the recipient to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of “Medium” in the resulting score.

(b) Applicability. This article applies to covered recipient information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, in accordance with the article entitled, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this award.

(c) Requirements. The Recipient shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at <https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171>, if necessary.

(d) Procedures. Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) () to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) Basic Assessments. A recipient may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800-171 against which the assessment was conducted.

(B) Organization conducting the assessment (e.g., Recipient self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD award—

(1) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and

(2) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.

(E) Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement).

(F) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Recipient shall use the following format for the report:

System Security Plan: _____

CAGE Code supported by this plan: _____

Brief description of the plan architecture: _____

Date of assessment: _____

Total Score Date score of 110 will achieved: _____

(2) Medium and High Assessments. DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

(ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, i.e., medium or high.

(vi) Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(e) Rebuttals.

(1) DoD will provide Medium and High Assessment summary level scores to the Recipient and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).

(2) Upon completion of each assessment, the recipient has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) Accessibility.

(1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Recipient for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

(3) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this article. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a recipient that is privileged or confidential).

(g) Subawards/Subcontracts.

(1) The Recipient shall insert the substance of this article, including this paragraph (g), in all subawards/subcontracts and other contractual instruments, including subawards/subcontracts for the acquisition of commercial products or commercial services (excluding commercially available off-the-shelf).

(2) The Recipient shall not award a subaward/subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with Safeguarding Covered Defense Information and Cyber Incident Reporting article, unless the subaward/subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in <https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171>, for all covered recipient information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subaward/subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subaward/subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to mailto:webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this article.

[] 35. SPACE OR FLIGHT TESTING AND EVALUATION (Feb 2024)

(a) The Recipient shall participate in and support the AFRL space/flight test process IAW AFRLI 61-103 (Parent ,Volume 1, and Volume 3), titled AFRL Research Test Review, Approval, and Oversight AND AFRL Flight Test and Evaluation AND AFRL Space Test and Operations, respectively.

(b) The Recipient will collaborate with the Government team (including AOTR and other identified personnel) to gather program space/flight test requirements.

(c) Participate in and support all reviews including the following by submitting briefing notes within fourteen (14) days prior to the start of the event:

(i) Space/Flight Test Planning Meeting (SFTPM)

(ii) Technical Review Board (TRB)

(iii) Safety Review Board (SRB)

(d) Develop a test plan and submit:

(i) A draft test plan to the Government eight (8) weeks prior to the start of testing

(ii) Submit final test plan five (5) weeks prior to the start of testing and two (2) weeks prior to the TRB

(iii) Update the test plan according to TRB results and resubmit to Government two (2) weeks prior to the SRB.

(iv) Update the test plan according to SRB results and resubmit to Government for Test Execution Authority (TEA)/ Flight Operations Authority (FOA) /Satellite Control Authority (SCA) approval.

(e) Adhere to the guidance referenced in paragraph (a) for unexpected events and mishaps. Utilize the AFRL Unexpected Event Worksheet included in AFRL 61-103 Volume 3. The Recipient shall report any unexpected events, including mishaps involving injury or damage to USAF personnel or property. If an AFRL representative is not present during the mishap, the Recipient shall notify the Government Technical Representative / Program Office or AFRL/DO of the mishap as soon as practicable after the mishap has been debriefed at the test location, but not later than eight (8) hours immediately following the mishap. If the Government Technical Representative / Program Office or AFRL/DO cannot be reached in person, the Recipient shall execute the alternate notification procedures as specified on the AFRL Unexpected Event Worksheet. In the event of a mishap, the data and information collected must be protected in accordance with guidance provided by a cognizant government representative. It is recommended that the Recipient have an established safety representative made known to the Government through whom communication will occur and the data and information collected will be transmitted.

(f) Coordinate with AOTR to provide the Government with any recorded data, analyses, and reports as required. The Government will review within fifteen (15) days with the final report due fifteen (15) days later.

(g) According to the guidance referenced in paragraph (a), document and provide RI Test Lead, AFRL/SE, and AFRL/DO with Lessons Learned at the conclusion of the space/flight test using AFRL RI Lessons Learned Worksheet within thirty (30) days after completion of the FLT testing. The Government will review within fifteen (15) days with the final report due fifteen (15) days later.

(h) The Recipient shall be bound by the operating procedures contained in the combined regulation/instruction entitled "Contractor's Flight and Ground Operations" (Air Force Instruction 10-220, Army Regulation 95-20, NAVAIR Instruction 3710.1 (Series), Coast Guard Instruction M13020.3, and Defense Contract Management Agency Instruction 8210.1) in effect on the date of this Agreement.

(i) In accordance with section 848 of the National Defense Authorization Act for Fiscal Year 2020, the Recipient shall not provide or use in the performance of this Agreement— (1) An unmanned aircraft system (UAS), or any related services or equipment, that (i) Is manufactured in the People's Republic of China or by an entity domiciled in the People's Republic of China; (ii) Uses flight controllers, radios, data

transmission devices, cameras, or gimbals manufactured in the People's Republic of China or by an entity domiciled in the People's Republic of China; (iii) Uses a ground control system or operating software developed in the People's Republic of China or by an entity domiciled in the People's Republic of China; or (iv) Uses network connectivity or data storage located in, or administered by an entity domiciled in, the People's Republic of China; or (2) A system for the detection or identification of a UAS, or any related services or equipment, that is manufactured (i) In the People's Republic of China; or (ii) By an entity domiciled in the People's Republic of China.

(j) The Recipient shall provide sufficient technical documentation and detail of the vehicle and modifications, of operator experience, safety and mishap history of the air vehicle, and design/procedural safety precautions to support the government independent airworthiness assessment and associated issuance of a Civil/Public Air Operations (CAO or PAO) Letter or Military Flight Release (MFR) or Test Approval Briefing (TAB) whichever is applicable. The Recipient shall support Government reviews conducted in the course of the airworthiness assessment process. The Recipient shall support Continuing Airworthiness Maintenance and Operations (M&O) on-site inspections or remote interviews conducted by the Government (as applicable).

(k) Subagreements. The Recipient shall insert the substance of this Article, including this paragraph (k), in all subagreements or other contractual instruments, including subagreements for the acquisition of commercial products or commercial services.

[X] 36. ADDRESSING DEI DISCRIMINATION BY FEDERAL RECIPIENTS (APR 2026)

(a) Definitions. As used in this article—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the recipient or subrecipient.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this agreement, the Recipient agrees as follows:

(1) The Recipient will not engage in any racially discriminatory DEI activities;

(2) The Recipient will furnish all information and reports, including providing access to books, records, and accounts, as required by the Grants Officer, for purposes of ascertaining compliance with this article;

(3) In the event of the Recipient's or a subrecipient's noncompliance with this article, this agreement may be canceled, terminated, or suspended in whole or in part, and the Recipient or subrecipient may be declared ineligible for further Government agreements;

(4) The Recipient will report any subrecipient's known or reasonably knowable conduct that may violate this article to the Grants Officer and take any appropriate remedial actions directed by the Grants Officer; and

(5) The Recipient will inform the Grants Officer if a subrecipient sues the Recipient and the suit puts at

issue, in any way, the validity of this article.

(6) The Recipient recognizes that compliance with the requirements of this agreement are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Recipient must include the substance of this article, including this paragraph (c), in subagreements at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

[X] 37. DISCLOSURE OF CONFLICT OF COMMITMENT AND CONFLICT OF INTEREST (JAN 2026)

(a) This award required that all current and pending research support, as defined by Section 223 of the FY21 National Defense Authorization Act to be disclosed at the time of proposal, for all covered individuals. Such disclosure will be updated annually during the performance of any research project selected for funding, and whenever covered individuals are added or identified as performing under this project. Covered Individuals are those who are listed as key personnel on proposals including but are not restricted to the principal investigator or co-principal investigator.

(b) Any decision to accept a proposal for funding under this announcement will include full reliance on the applicant's statements. Failure to report fully and completely all sources of project support and outside positions and affiliations may be considered a materials statement within the meaning of the federal False Claims Act and constitute a violation of law.

(c) The funding agency was required to conduct a Pre-Award conflict of interest/conflict of commitment review of any proposal selected for funding, as defined in the National Security Strategy for United States Government-Supported Research and Development (NSPM-33) and the DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions. Offerors are advised that any significant conflict of interest/conflict of commitment identified may be a basis for the rejection of an otherwise awardable proposal. Be further advised and aware that none of the funds authorized to be appropriated or otherwise made available for the DoD for fiscal year (FY) 2025 may be obligated or expended to award a grant, contract, or other assistance to an institution of higher education for the specific purposes of conducting fundamental research in collaboration with a covered entity that is included on the most recent version of the list developed pursuant to section 1286 of the National Defense Authorization Act (NDAA) for FY 2019, as amended, or to any employees of such institutions. Similarly, the DoD is prohibited from providing funding to or making an award of a fundamental research project proposal in which a covered individual is participating in a malign foreign talent recruitment program. No U.S. institution of higher education that hosts a Confucius Institute may receive DoD funds.

(1) General Requirement for Disclosure: You and your organization must disclose any potential or actual scientific or non-scientific Conflict of Interest(s) to us. You must also disclose any potential or actual conflict(s) of interest for any subrecipient you include in your proposal. You and your organization must disclose within five (5) business days of awareness. You must provide enough information for us to evaluate your disclosure. We may have to ask you more questions if we need more information. At our discretion, we may ask you for a conflict-of-interest mitigation plan after you submit your proposal. Your plan is subject to our approval.

(2) Scientific Conflict of Interest: Scientific collaborations on research and development projects are generally the result of close collaboration prior to the submission of applications for support. Accordingly, virtually all of these collaborations might be considered to include a potential conflict of

interest. The potential conflict is mitigated by the disclosure of these collaborations, and the list of current and pending support you provide for senior and key researchers.

[X] 38. AFOSR-SPECIFIC SECURITY RISK REVIEW INFORMATION (JAN 2026)

(a) Security Risk Review. Each proposal submission was subject to a Risk-based Security Review prior to selection for award. The Risk-based Security Review is applied to federally funded research designed to help protect Department of the Air Force Science and Technology (S&T) by identifying possible vectors of undue foreign influence. AFRL will follow all policy and procedures outlined in Air Force Research Laboratory (AFRL) Instruction AFRLI 61-113, Science and Technology Protection for the Air Force Research Laboratory and Department of the Air Force Instruction DAFI 63-101/20-101, Integrated Lifecycle Management. The Risk based Security Review will be conducted in accordance with OUSD(R&E)'s "Policy for Risk Based Security Reviews of Fundamental Research" and the most updated Decision Matrix.

(b) Security risk review was developed for all proposed Senior/Key personnel and "Covered Individuals." These risk reviews were based on information disclosed in a Research and Related Senior and Key Person Profile and Security Questionnaire. In addition, any accompanying or referenced documents, and publicly available information, will be utilized in risk reviews as well as classified information. Nationality or citizenship are not factors in the security risk reviews.

(c) External Engagements. When considering all external engagements, AFRL incorporates a holistic decision making process that encompasses technical and security factors. The security review method implemented by AFRL measures risk factors to identify the appropriate Risk Acceptance Level (RAL) within the organization. The objective analysis of the security risk factors is conducted to empower AFRL's S&T leaders to make risk informed decisions. The review process looks at the risk factors indicated in the most recent DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions.

[X] 39. ACTIONS REQUIRED BY COVERED INDIVIDUALS (JAN 2026)

(a) Covered Individual. An individual who contributes to a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a federal research agency; and is designated as a covered individual by the federal research agency concerned. See 42 U.S.C. § 6605, Definitions.

(b) Federal law requires that all current and pending research support, as defined by 42 U.S.C. §6605, must be disclosed at the time of proposal submission, for all covered individuals. If the position is outlined in the proposal, AFOSR views this as a covered individual. The Government may require an updated disclosure during the performance of any research project selected for funding. The Government will require an updated disclosure whenever covered individuals are added or identified as performing under the funded project.

(c) Covered Individuals are also required to sign the "Privacy Act Statement" and provide such signed statement to the Applicant/Recipient for submission with the proposal.

[X] 40. ACTIONS REQUIRED BY RECIPIENTS DURING PERIOD OF PERFORMANCE (JAN 2026)

(a) Recipient will utilize a section of the Research Progress Performance Report (RPPR) to provide disclosure updates for Senior/Key Research Personnel. In addition, whenever a new covered individual(s) is to be added or identified as performing under the funded project, a new Research and Related Senior and Key Person Profile will be required prior to continued performance.

(b) If, at any time, during performance of this award, the Recipient learns that its Senior/Key Research Personnel (including any sub-awardee personnel who receive this designation) are or are believed to be participants in a Foreign Government Talent Program or have Foreign Components with a strategic competitor or country with a history of targeting U.S. technology for unauthorized transfer, the Recipient will notify the Contracting/Grants/Agreements Officer within five (5) business days of awareness.

(c) This disclosure must include specific information as to the personnel involved and the nature of the situation and relationship. The Government will review this information and conduct any necessary fact-finding or discussion with the Recipient. The Government's determination on disclosure may include acceptance, mitigation, or termination of the award. The Recipient will be required to flow down this provision to all sub-awardees who have personnel designated as Senior/Key Research Personnel as a result of their involvement in the performance of the research.

[] 41. DURIP-SPECIFIC REQUIREMENTS (Apr 2024)

(a) This grant is issued under the Defense University Research Instrumentation Program (DURIP) to augment current or develop new research capabilities in support of research relevant to the Department of Defense (DoD).

(1) Funds received under this award may be used for:

(i) Acquisition of major equipment or instrumentation approved consistent with the evaluation and selection criteria in the program announcement, including: reasonable costs for design, construction, assembly; and/or, installation by external contractors or university technicians or engineers

(ii) Computers for DoD-relevant research programs approved consistent with the evaluation and selection criteria in the program announcement

(iii) Travel costs for testing and/or acceptance of proposed instrumentation, and associated indirect Facilities & Administrative (F&A) costs

(2) Funds received under this award must not be used for:

(i) Construction or modification of buildings; building support systems such as heating, ventilation, air conditioning, plumbing, or electrical; or fixed equipment such as clean rooms or fume hoods

(ii) Costs for continued operation and maintenance, including extended warranties

(iii) Purely instructional equipment

(iv) General purpose computing facilities

(v) Direct salaries of faculty, postdoctoral associates, or students

(vi) Costs that are not allowable under 2 CFR 200 Subpart E - Cost Principles

(b) DURIP equipment must be ordered promptly.

(1) Equipment orders should be placed as quickly as practicable after you receive this award. It is expected that all equipment is in place by the end of the period of performance. If there are any delays, you must contact the Grants Officer at least 30 days before award expiration to negotiate a resolution.

(c) Interim Performance reports are not required unless specified in the Reporting Information section of the grant.

(d) The Final Performance Report is replaced by a Final Equipment Report.

(1) The final Equipment Report shall:

(i) Identify the acquired equipment (although it may vary from that described in your proposal) by name and associated costs, and

(ii) summarize the research or educational project for which the equipment will be used.

[] 42. CONFERENCE/WORKSHOP SPECIFIC REQUIREMENTS (Apr 2024)

(a) Interim Performance reports are not required unless specified in the Reporting Information section of the grant.

(a) The Final Performance Report is replaced by a Final Conference Report.

(b) The final Conference Report shall contain a summary of all scientific papers presented and a list of all attendees.