Date: 20260730

Research and Technology Protection (RTP) and Security

1. Research and Technology Protection (RTP)

Work under the NGA BAA is expected to fall between TRL 1 and TRL 6

Proposals eligible for award will undergo a Security evaluation.

Due Diligence and Research Security Program Requirements

NGA will conduct risk-based security reviews of the required disclosures in accordance with the Department of War (DoW) Policy for Risk-Based Security Reviews of Fundamental Research to identify practices or behaviors identified in Table 1 of the *2026 DoW Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions*, or subsequent revisions. Please see the following link for more information on disclosure and review requirements: https://basicresearch.defense.gov/Programs/Academic-Research-Security/

NGA's analysis of affiliations and associations of covered individuals is compliant with Title VI of the Civil Rights Act of 1964. Information regarding race, color, or national origin is not collected and does not have bearing in NGA's assessment.

As Fundamental Research, proposals submitted in response to Topic Calls under the NGA BAA shall comply with the following requirements:

(1) Reporting Potential Conflicts of Interest and Commitment.

Awardee agrees to promptly report to NGA any and all indicators identified in *DoW Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions* for a risk-based security review for potential conflicts of interest and commitment. Notifications may be sent by email to the BAA Program Management Office (PMO) BIGST_BAA_PMO@nga.mil. NGA reserves the right to invoke DoW R&D General Terms and Conditions OAR Article III. 'Remedies and termination' for any unmitigated risk factors identified during NGA risk-based security reviews of required disclosures and annual verification of RPPR submissions.

(2) Research Security Training Requirement

In accordance with the CHIPS and Science Act of 2022 (P.L. 117-167), each covered individual listed on an NGA grant application must certify that they have completed Research Security Training (RST) within 12 months of the date of application submission. This individual certification is required at the time of the application submission, through the Biographical Sketch. The Act also requires applicant institutions to certify that each covered individual who is employed by the institution and listed on the application has completed RST. Completion of RST

and the individual and institutional certifications is required for applications submitted no more than 12 months after contract award.

Proposing organizations must certify the completion of this training for all covered individuals by checking box number 17 on the SF-424, "Application for Federal Financial Assistance," with the following language:

> *"By submitting this application, the proposer's research institution Authorized Organizational Representative (AOR) certifies that all key personnel have completed the Federally mandated research security training (RST). The National Science Foundation (NSF), in partnership with the National Institutes of Health (NIH), the Department of Energy (DOE) and the Department of War (DoW), has provided four online research security training modules as a resource to awardee organizations. Subsequently, the Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE) Center developed an updated and condensed version of the four modules. The condensed RST module is designed to meet the Government-wide RST requirement in section 10634 of the CHIPS and Science Act of 2022 (as in 42 U.S.C. § 19234). To that end, NSF, NIH, DOE, and DoW all recognize completion of the condensed module as compliant with their respective RST requirements."*

Proposers may use any training that aligns with the guidelines set forth by the Executive Office of the President's Office of Science and Technology Policy, covering topics such as cybersecurity, international collaboration, foreign interference, and rules for the proper use of funds, disclosure, conflict of commitment, and conflict of interest. The condensed training modules developed by the NSF-funded SECURE Center are encouraged and available at https://www.secure-center.org/resources.

(3) Research Security Program

The proposing institution must establish and maintain a research security program in accordance with National Security Presidential Memorandum 33 (NSPM-33), including disclosure to NGA of any changes to submitted common disclosure forms, change of covered individuals, and any indicators of participation in a Malign Foreign Talent Recruitment Program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.

(4) Flow Down

The performer or recipient must flow down all research security requirements, including submission of common disclosure forms, to any sub-tier contracts or agreements involving covered individuals with direct participation in the performance of the research.

Submission of Common Disclosure Forms for Fundamental Research

The Common Disclosure Forms shall only be submitted upon NGA's request after proposal selection.

Awards which cover fundamental research funded by the DoW, regardless of award instrument or type of proposing entity, are required to submit certified Common Disclosure Forms for each covered individual (See NGA BAA Attachment J: Definitions).

In accordance with NSPM-33, "Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education", dated 29 June 2023, and section 10632(a)(1) of the CHIPS and Science Act of 2022 (Public Law 117-167), NGA will request the submission of two (2) Common Disclosure forms (CDFs) for each covered individual after a proposal is selected for award and annually thereafter. DoW Grant Information Notice (GIN 24-01) requires the collection of digital persistent identifiers (DPI) from covered individuals on proposals for assistance awards.

Awardee agrees to submit initial and annual verification and updates to the CDFs for each covered individual no later than two hundred seventy-five (275) days prior to the start of the reporting period.

1) Common Form for Biographical Sketch.
2) Common Form for Current and Pending (Other) Support Information.

The link to these forms is at: NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Requirements & Standardization (nsf.gov)

It is vital that submission of such disclosure information be taken seriously. Failure to comply with terms and conditions related to disclosure requirements may cause NGA to take action(s) to remedy non-compliance, such as disallowing costs, withholding of further awards, or wholly or partly suspending the grant, pending corrective action Further, violations that are potentially criminal will be referred to the NGA Inspector General, the Department of Justice, or other law enforcement agencies, as appropriate.

Evaluation of Common Disclosure Forms for Fundamental Research

(4) Mitigations

Based on the results of a risk-based security review of required disclosures and annual verification of RPPR submissions, Awardee and NGA may have the opportunity to negotiate strategies to mitigate the potential risk posed by discouraged practices or behaviors. In cases where NGA and Awardee are unable to come to an agreement concerning proposed mitigation strategies, NGA reserves the right to invoke DoW R&D General Terms and Conditions OAR Article III. 'Remedies and termination' for any unmitigated risk factors associated with

prohibited or discouraged actions identified in this addendum or the *DoW Component Decision Matrix to Information Fundamental Research Proposal Mitigation Decisions*.

Upon conclusion of the negotiations, if NGA determines, despite any proposed mitigation terms (e.g. mitigation plan, alternative research personnel), the participation of any covered individuals still represents unacceptable risk to the program, or proposed mitigation affects the Government's confidence in the proposer's capability to successfully complete the research (e.g., less qualified covered individuals) the Government may determine not to award the proposed effort. Any decision not to award will be predicated upon reasonable disclosure of the pertinent facts and reasonable discussion of any possible alternatives while balancing program award timeline requirements.

Congruent with executive, congressional, and departmental direction, NGA may decline award to an Offeror when:

1. The Offeror
   - **(a)** fails to provide digital persistent identifiers (DPI) from covered individuals on common disclosure forms as required by DoW Grant Information Notice (GIN) 24-01;
   - **(b)** fails to certify that covered individuals have completed Research Security Training (RST) within 12 months of the date of application submission or RPPR submission;
   - **(c)** receives federal funds in excess of $50 million per year and has not established a research security program in accordance with National Security Presidential Memorandum 33 (NSPM-33);
   - **(d)** Awardee hosts a Confucius Institute (as defined in the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2024), or a cultural institute established as a partnership between the Awardee and a Chinese institution of higher education to promote and teach Chinese language and culture that is funded, directly or indirectly, by the Government of the People's Republic of China, unless the proposer has been issued a waiver by the Secretary of Defense pursuant to section 1062 of the William M. (Mac) Thornberry National Defense Authorization Act for FY 2021;
   - **(e)** has indicators of prohibited factors listed on the "2026 DoW Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions", or subsequent revisions;
   - **(f)** has a documented history of patent or intellectual property theft;
   - **(g)** has a covered individual who is published on the list under section 1237(b) of the Strom Thurmond NDAA for FY 1999 (Public Law 105-261; 50 U.S.C. 1701 note.); or
   - **(h)** does not have a policy or procedure addressing MFTRPs; or
2. The Offeror, its parent company or its subsidiary is:
   - **(a)** located in a foreign country of concern (FCOC); or

(b) has an owner or covered individual that has a foreign affiliation with a research institution located in a FCOC; or

(c) has an owner or covered individual that is party to a MFTRP; and

3. The relationships and commitments described in clauses 2(a) through 2(c):
   (a) interfere with NGA's capacity to carry out activities it supports.
   (b) create duplication with DoW-supported activities.
   (c) present concerns about conflicts of interest (CoI) or commitment (CoC).
   (d) were not appropriately disclosed to NGA.
   (e) violate Federal law or NGA terms and conditions.
   (f) pose a risk to national security.

Discouraged Actions.

Unless the Awardee has been issued a waiver by the Director, NGA, or higher authority, the Awardee and all covered individuals are discouraged from engaging in any practices or behaviors identified in Table 1 of the *DoW Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions* , or collaborations and commitments identified by NGA implementing rules and regulations including, but not limited to:

1) any entity or individual listed on the Prohibited Entity Lists

2) any entity identified on the Transportation Security Administration's No Fly List;

3) any entity identified on the Federal Bureau of Investigation's Terrorist Screening Center (TSC) Terrorism Watchlist;

4) any of the "Seven Sons of National Defense" (国防七子) Schools or State Key Laboratories:

a. Beihang University (北京航空航天大学), previously known as the Beijing University of Aeronautics and Astronautics (BUAA);
b. Beijing Institute of Technology (北京理工大学);
c. Nanjing University of Aeronautics and Astronautics (南京航空航天大学);
d. Nanjing University of Science and Technology (南京理工大学);
e. Northwestern Polytechnical University (西北工业大学);
f. Harbin Institute of Technology (哈尔滨工业大学);
g. Harbin Engineering University (哈尔滨工程大学);
h. State Key Laboratory for Underwater Information and Control;
i. Multi-hull Ship Technology Key Laboratory of Fundamental Science for National Defense;
j. National Key Laboratory of Underwater Acoustic Technology;
k. National Defense Key Laboratory of Underwater Vehicles Technology;

5) Any of the "Seven Sons of Ordnance Industry" (兵工七子) Schools;
a. Beijing Institute of Technology (北京理工大学)

b. Nanjing University of Science and Technology (南京理工大学)
c. Shenyang Ligong University (沈阳理工大学)
d. North University of China (中北大学)
e. Chongqing University of Technology (重庆理工大学)
f. Changchun University of Science and Technology (长春理工大学)
g. Xi'an Technological University (西安工业大学)

6) Any organ of the armed forces of a Foreign Country of Concern (FCOC) (e.g., People's Liberation Army, Armed Forces of the Russian Federation, Islamic Republic of Iran Armed Forces, Korean People's Army, etc.);

7) State-owned Enterprise Defense Conglomerates;

8) People's Republic of China's State Administration for Science, Technology, and Industry for National Defense (SASTIND) schools; or

9) Any collaborations or commitments that the Risk Review Board determines

a. interfere with the capacity for activities supported by NGA to be carried out;
b. were not appropriately disclosed to NGA on the common disclosure forms (OMB Number 3145-0279) at award initiation and annually thereafter;
c. violate Federal law or terms and conditions of contracts or other agreements awarded by NGA; or
d. pose a risk to national security.

Program Protection Implementation Plan (PPIP)

For proposals selected for funding that require a PPIP, the Government will require submission of a PPIP in the government-provided templated format (see RTP_SEC_Attch7_PPIP_Template.docx) and review the PPIP to determine the proposer's ability to identify and protect technology elements essential to meet topic-specific requirements in accordance with DoDI 5000.83 and the DoD Technology and Program Protection (TPP) Guidebook.

The PPIP Template must be submitted by the applicant after receiving notification of proposal selection for funding. Applicant (Offeror) must provide a completed form if requested by NGA.

NGA will work with the potential awardee to submit a PPIP that meets protection requirements within five (5) sections. The following table describes the requirements that each section must meet:

SUBFACTOR	Requirement
1. Introduction, Updates, and Responsible Points of Contact (POCs)	The PPIP (1) describes the purpose of the program that will be addressed by the PPIP; and (2) identifies the lead prime and subcontractor personnel responsible for implementing countermeasures described in the PPIP.
2. Technology Element Identification and Impact Assessment	The PPIP sufficiently demonstrates (1) how the proposer will conduct, validate, and maintain Critical Technology Element (CTE) assessments for all development activities throughout the program lifecycle; including (2) how technologies are selected as critical; and (3) reasons why other technologies are not selected as critical.
3. Identified Threats and Vulnerabilities	The PPIP sufficiently describes the process for identifying and assessing (1) threats and (2) vulnerabilities specific to CTE or assessed as more likely given the program's content or intent, including (3) what sources will inform identification and assessment and (4) how the proposer will maintain awareness of emerging threats and vulnerabilities throughout the program lifecycle.
4. Countermeasures and Risk Mitigation Plan	The PPIP sufficiently describes (1) how the proposer plans to address Section 4, "Countermeasures and Risk Mitigation Plan," of Attachment 9 of Appendix 2; or (2) why a given subsection is not applicable given the program's content or intent.
5. Response, Recovery, and Support	The PPIP sufficiently (1) identifies the lead prime and subcontractor personnel responsible for response coordination; and sufficiently describes (2) reporting and (3) remediation policies necessary to address Section 5, "Response, Recovery, and Support," of Attachment 9 of Appendix 2.

For proposals that involve elements of testing or evaluation that require an exception to outlined protection requirements, an optional Government Test Plan Template is provided (see RTP_SEC_AttchC-8_Security_Test_PlanTemplateV2.0.docx); it sufficiently covers most testing, experimentation, evaluation scenarios and associated risk mitigations.

Topic-Specific Mitigations

[PLACEHOLDER for risk mitigations from RAD]

Counterintelligence (CI) Awareness Briefings

(a) Government Briefings. NGA reserves the right to provide CI awareness briefings to Contractor personnel performing work under this contract. Upon written notification from the Government, the Contractor shall permit authorized NGA Counterintelligence personnel to conduct such briefings at Contractor facilities where work under this contract is performed.

(b) Advance Notification. The NGA shall provide the Contractor not less than thirty (30) business days advance written notice prior to conducting a CI awareness briefing under this clause.

(c) Scheduling. To minimize disruption to Contractor operations, CI awareness briefings conducted under this clause shall:

1. Be scheduled Monday through Friday only;
2. Occur between the hours of 0900 and 1600 local time;
3. Not be scheduled on Federal holidays;
4. Be coordinated in advance with a Contractor-designated point of contact.

(d) Nature of Visit. CI awareness briefings conducted pursuant to this clause are intended solely for information-sharing and protective awareness purposes and shall not constitute inspections, audits, or compliance reviews of the Contractor's facility or operations.

(e) Contractor Support. The Contractor shall:

1. Provide reasonable access to a suitable meeting space for the briefing;
2. Coordinate scheduling with the Government-designated representative;
3. Make reasonable efforts to ensure maximum practical participation of Contractor personnel performing work under this contract;
4. Distribute Government-provided CI awareness materials to personnel unable to attend the briefing, when such materials are provided.

(f) Duration and Scope. The Government will make reasonable efforts to limit the duration and scope of CI awareness visits to the time necessary to conduct the briefing and respond to questions from Contractor personnel.

(g) Coordination. The Government and Contractor shall coordinate in good faith to ensure that CI awareness briefings are conducted in a manner that minimizes disruption to ongoing contract performance.

2. Security

Each Topic will have security requirements for information and personnel. Attachments RTP_SEC_Attch1-6 contain security language for unclassified, unclassified CUI and classified programs. The Offeror must comply with the appropriate requirements based on classification of the Topic Call. The attached documents provide information regarding the following sections:

- Work Performance Security Requirements
- Personnel Security Requirements
- Physical Security Requirements
- Information Security Requirements

Unclassified Work Performance Security Requirements

If applicable, and when approved in writing by the COR, uncleared Contractor personnel are authorized to work on this contract at the Unclassified level, with access up to DoD Controlled Unclassified Information (CUI) at the Contractor site without the requirement of a security clearance.

Uncleared Personnel Security Requirements

If applicable, and when approved in writing by the COR any Contractor personnel working with CUI information must receive a favorable HSPD-12 and/or HSPD-12 Tier 1 adjudication prior to accessing CUI information. Contractor personnel who require access to CUI for 60 days or less must receive a favorable HSPD-12 adjudication. Contractor personnel who require CUI access for more than 60 days must receive a favorable HSPD-12 Tier 1 adjudication. NGA will sponsor the HSPD-12 and HSPD-12 Tier 1 background investigation for Contractor personnel as needed.

Foreign nationals are not permitted to perform unclassified work under the terms of this contract without prior written approval from the Contracting Officer (CO) or the COR. Should NGA identify the use of unauthorized personnel, the CO may direct the Contractor, at its own expense, to remove and replace any unauthorized Contractors, Subcontractors, or other personnel performing on the contract. Such action may be taken at the NGA's discretion without prejudice to its rights under any other contract provision, e.g., termination for default.

Uncleared Contractor personnel visiting NGA facilities or other sites may receive the appropriate visitor badge and be escorted, as appropriate. The Contractor will return the visitor badge at the end of each visit day.

Foreign Participation

Each Topic will specify whether non-U.S. organizations and/or individuals may participate and any specific controls or security regulations that apply. If allowable under the Topic, any and all forms of foreign participation must be clearly and fully disclosed within the proposal. For controlled unclassified information (CUI) and classified submissions, this includes disclosing

and mitigating any Foreign Ownership Control and Influence (FOCI) issues prior to transmitting the submission to NGA. Additional information on FOCI can be found at https://www.dcsa.mil/mc/isd/foci/.

Upon written approval from the CO or the COR, non-U.S. organizations and/or individuals may participate to the extent that such participants comply with any necessary nondisclosure agreements, security regulations, export control laws, and other governing statutes applicable under the circumstances.

Classified Work Performance Security Requirements

Contractors must abide by the DD Form 254 - Contract Security Classification Specification (referred to as DD254 hereafter), the National Industrial Security Program Operating Manual (NISPOM 32 CFR Part 117), and all other applicable security policies and regulations including operational security (OPSEC) requirements.

Some personnel may need to obtain access to Special Access Program (SAP), and/or Control Access Program (CAP) and/or Alternate Compensatory Control Measures (ACCM) Information as required for the execution of NGA's sensitive program missions. Access will not be granted without written permission from the COR.

Defense Counterintelligence and Security Agency (DCSA) remains the Cognizant Security Agency (CSA) for individuals performing work with collateral (SECRET or TOP SECRET) security clearances. As such, Security Executive Agent Directive (SEAD) 3 reporting should continue to be provided to the Contractor's Facility Security Officer (FSO) for reporting to DCSA via Defense Information Security System (DISS). DCSA will also dictate mandatory security training as the CSA for the collateral cleared community.

Personnel Security Requirements

Contractor personnel performing Top Secret/Sensitive Compartmented Information (TS/SCI) work on the contract are required to have active TS/SCI clearances for access to TS/SCI facilities, when performing duties within TS/SCI environments, and for access to TS/SCI computer systems for the performance of this contract. Contractors are subject to a Counterintelligence-Scope Polygraph examination, as requested by NGA. As a condition of employment and assignment, contractors who have not successfully completed polygraph testing within the last five years must immediately schedule a polygraph examination and must complete the process, in no more than three test sessions, within 90 days.

All Contractor personnel shall possess a current Top Secret Personnel Security Clearance and be eligible for favorable NGA adjudication for SCI access. The government will be responsible for verifying security clearances/SCI eligibility of the Contractor personnel in accordance with (IAW) SEAD 7: "Reciprocity of Background Investigations and National Security Adjudications". If needed, NGA will sponsor SCI accesses at its sole discretion. NGA will

provide badges, Common Access Cards (CAC) and other items (e.g. parking hangtags) when applicable, for required Contractor personnel.

Upon onboarding, all cleared NGA contractors shall be enrolled into the NGA Continuous Vetting program and the Office of Director of National Intelligence Continuous Evaluation System IAW SEAD 6: "Continuous Evaluation" and Trusted Workforce (TW) 2.0 requirements. Cleared NGA contractors must report new applicable security issues, new foreign travel/contacts, and other required information to their FSO and NGA personnel security IAW SEAD 3: "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position" and NGA Instruction 5205.3: "Security Reporting Requirements". Additionally, cleared NGA contractors will be required to be enrolled into a Report of Arrest and Prosecution Background (RAPBack) program, which also complies with TW 2.0 requirements.

Cleared NGA contractors who are designated to participate in NGA's annual Security Financial Disclosure Program (SFDP) must comply IAW with NGA SFDP requirements.

The Contractor shall inform NGA as soon as practicable when its employees will no longer support the contract (see DD254). NGA desires notification prior to the day the individual no longer supports the contract but requires notification no later than the day that contract support ends. If Contractor personnel will no longer be supporting NGA via an NGA contract, NGA shall take all appropriate action, up to and including debriefing the contractor from SCI access and terminating logical and physical access to NGA IT systems and facilities.

Upon notifying NGA that a Contractor will no longer support the contract, the Contractor must return all NGA Badges, CAC, hangtag, and any other government furnished property. These items can be returned to the NGA Workforce Support Center, NGA Site Security Office, or the Contracting Officer Representative (COR) as soon as practicable, but no later than four (4) business days from the date of Contractor departure.

When Contractor personnel are unable to turn these items into the NGA Workforce Support Center, NGA Site Security Office, or COR then it is the responsibility of the Contractor's FSO to collect the items from the individual and return them to NGA as soon as practicable, but no later than four (4) business days from the date of Contractor departure.

If the FSO debriefs their employee, the FSO shall provide a copy of the debriefing statement, plus all applicable Government-furnished items (e.g. NGA Badge, CAC, Courier Card, parking hangtags, etc.) to the NGA Site Security Office or the NGA Workforce Support Center as soon as practicable, but no later than four (4) business days from the date of Contractor departure.

Physical Security Requirements

All classified work performed at a non-NGA facility must be approved by the COR. Any classified work performed at contractor sites must be performed in either an NGA accredited SCIF, Other Government Agency (OGA) SCIF, or an approved secure collateral space that has either a Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), Joint Use Agreement or Co-Use Agreement with NGA for this contract. SCIF or secure facility

accreditation shall be at least the level commensurate with the level of safeguarding required by the contract DD254.

Pursuant to "IC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities Version 1.5.1; IC Tech Specs for ICD/ICS 705", the NGA accrediting official, or designee, shall conduct periodic security inspections/reviews to ensure the efficiency of NGA accredited SCIF operations, identify deficiencies, and document corrective actions taken. Inspections/reviews of NGA accredited SCIFs shall be conducted based on threat, facility modifications, sensitivity of programs, past security performance, or at least every five years. Technical Surveillance Countermeasures (TSCM) activities in NGA accredited SCIFs will only be conducted by NGA TSCM teams consisting of NGA military, civilian, or contractor personnel who have successfully completed approved TSCM training. Authorized inspectors shall be admitted to a SCIF without delay or hindrance when inspection personnel are properly certified to have the appropriate level of security clearance and SCI indoctrination for the security level of the SCIF.

Contractor personnel are forbidden from bringing prohibited or unauthorized items into any NGA installation or other secure facility covered under this contract. These items include weapons, cell phones, cameras, two-way pagers, laptops, recording devices of any kind, flash drives, or any other removable media. Exceptions may be granted by NGA Security upon the Contractor's request. If granted, Contractor personnel must bring documentation showing approval prior to entering with the item(s). Violations may subject the Contractor and its offending personnel to civil and/or criminal liability IAW applicable laws and regulations governing access to secure Government facilities.

Information Security Requirements

NGA shall have the sole authority to determine whether, and to what extent, protected information shall be provided to the Contractor under the terms of the contract. Access to classified information will be pursuant to the security requirements established in the DD254. The Contractor shall not access, download, print, or further disseminate any classified information outside the execution of the defined contract requirements without the guidance and written permission from the COR.

When the Contractor receives protected information under the terms of this contract, the Contractor will comply with all applicable NGA, DoD, and IC information security policies (including the Consolidated NGA (CoNGA) Security Classification Guide) for the proper marking, handling, processing, storing, and safeguarding of classified and unclassified material. The Contractor will ensure that document markings are given the lowest possible security classification to maximize dissemination while still maintaining the information's confidentiality and integrity as necessary.

Access to CUI will be pursuant to DFARS clause 252.204.7012. The prime contractor shall include this clause, including paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to

identify the parties. The Contractor shall determine if the information required for Subcontractor performance retains its identity as covered defense information and will require protection under this clause. Contractor personnel shall not release any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless the COR has given prior written approval or in performance of a project that has been scoped and negotiated by NGA.

NGA will assess and authorize Contractors to process classified information on government-owned information systems, conduct oversight of such information system processing, and provide information system security guidelines IAW with FAR clause 52.204-21 and other information system security control policies, standards, and procedures. Contractor will be responsible for executing specific provisions under the contract for the accreditation of classified information systems, and upon request, shall provide the COR a written statement confirming accreditation compliance with the minimum information systems requirements established in the DD254. The Contractor shall include the substance of FAR clause 52.204-21 in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items), in which the Subcontractor may have federal contract information residing in or transiting through its information system.

In accordance with FAR Part 4.7 and FAR clause 52.215-2, the Contractor may retain one archival copy of any Government-furnished information provided to the Contractor during the course of performance of the contract, subject to Contractor following relevant data safeguarding practices and CUI restrictions. The disposition of such Government-furnished information is otherwise solely at the discretion of the Government. As directed by the NGA CO or COR, the Contractor will destroy or return to NGA all Government-furnished information upon contract termination or when no longer required for contract performance.

In situations when electronic transmission is not practicable, Cleared Contractor personnel may hand-carry contract-related classified information when authorized by the COR in writing. Approved Contractor personnel must obtain NGA courier authorization prior to hand-carrying of classified contract-related information. Only classified information related to the performance of this contract may be hand-carried. Contractor personnel will be limited to hand-carrying classified information between approved Contractor facilities and US Government facilities unless the COR approves other circumstances in writing, when applicable, on a case-by-case basis.

Cybersecurity Requirements

The Contractor must, at a minimum, implement 10 U.S.C. Sections 391 and 393 along with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” requirements.

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor 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/)
In the event that the Contractor discovers a cyber incident that affects a covered Contractor information system or covered defense information residing therein, or that affects the Contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

1. Notify the DoD Cyber Crime Center (DC3) and the COR in writing within 72 hours of incident discovery

2. 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 Contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor'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 Contractor's ability to provide operationally critical support.

In the event the Contractor discovers and isolates malicious software in connection with a reported cyber incident, the Contractor shall submit the malicious software to DC3 in accordance with instructions provided by the COR. The Contractor should NOT send the malicious software to the COR.

Insider Threat Requirements

Contractor will establish and maintain an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" and Presidential Memorandum "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs." As soon as practicable, Contractor shall report to the COR events that may have an effect on the status of the entity's or an employee's eligibility for access to classified information; report events that indicate an insider threat to classified information or to employees with access to classified information; report events that affect proper safeguarding of classified information; and report events that indicate classified information has been, or is suspected to be, lost or compromised.

Public Disclosure of Scientific and Technical Information

a. The Recipient may make formal public disclosure of the scientific and technical information from fundamental research (e.g., release articles for appropriate professional publications or present papers at scientific meetings or symposia) and will take the following steps:

(1) A copy of the article, paper, report, etc., shall be provided to the Government for review 45 days prior to submission for publication. The article should be sent by email to the BAA PMO (BIGST_BAA_PMO@nga.mil).

(2) Unless otherwise notified by the Program Office after review of the paper, please comply with the following:

- All images and graphics used in a paper / presentation need to be cited. In a PowerPoint presentation we would suggest adding a statement at the end stating all images are self-produced.

- Include reference to the National Geospatial-Intelligence Agency and grant number in any Acknowledgements.

- Do not use the NGA seal or logo on any documents or PowerPoint presentations.

- Do not depict, show, or list NGA personnel or facilities.

- Make sure that there are no placeholders in the submitted article. The Public Release Office will send it back to get the final image or numbers which delays the approval.

- Papers over 25 pages will take the full 45 business days to complete.

- Send a copy of the NGA approved (for public release), final published article or manuscript to the Program Office.

(3) Consistent with DoW Fundamental Research Guidance, dated 25 August 2025, NGA will not restrict disclosure of the results of fundamental research, except when required by applicable federal statutes, regulations, or executive orders. Accordingly, NGA's pre-publication review is intended, inter alia, to confirm: a) acknowledgement of NGA sponsorship through inclusion of the grant number; b) that the NGA logo has not been used; c) that NGA personnel or facilities are not shown or listed; d) that no sensitive or confidential information of NGA is included; and e) compliance with applicable federal laws, regulations, and policy.

b. The Recipient may utilize the scientific and technical information resulting from this grant work in consulting or discussing this and related information with other qualified individuals or groups of individuals, where appropriate, for furthering this research and/or development effort.

Public Acknowledgement Requirement

To ensure consistent and searchable acknowledgment of DoW funding, recipients of DoW R&D funds are required to include the following language in all public documents pertaining to the funded work:

This work was funded by the Department of War, [name of the funding agency or office] under award number [specific DoW grant number(s) in this format: XXXXXX-FY-N-XXXX], as part of a financial assistance award totaling $XX.

If the work was funded by more than one DoW award, the following language should be used:

This work was funded by the Department of War, [name of the funding agency or office] under award number [specific DoD grant number(s) in this format: XXXXXX-FY-N-XXXX] as part of a financial assistance award totaling $XX and [name of the funding agency or office] under award number [specific DoWgrant number(s) in this format: XXXXXX-FY-N-XXXX] as part of a financial assistance award totaling $XX.

Unauthorized Use of NGA Name, Seal and Initials

a. As provided in 10 U.S.C. Section 425, no person may, except with the written permission of both the Secretary of Defense and the Director of National Intelligence, knowingly use the words "National Geospatial-Intelligence Agency", "National Imagery and Mapping Agency", or "Defense Mapping Agency," the initials "NGA", "NIMA" or "DMA," the seal of National Geospatial-Intelligence Agency, National Imagery and Mapping Agency, or the Defense Mapping Agency, or any colorable imitation of such words, initials, or seal in connection with any merchandise, retail product, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Secretary of Defense and the Director of National Intelligence.

b. Whenever it appears to the Attorney General that any person is engaged or about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to hearing and determination of such action and may, at any time before final determination, enter restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

Reporting Changes in Fundamental Research Designation

Fundamental research funded by the DoW includes the intent to publish and share results openly and should not be subjected to approval-based publication constraints. NGA does not expect that the research or results will require restrictions on their dissemination. Appendix B of the Under Secretary of War for Research and Engineering's S&T Protection Guide contains a Fundamental Research Review to assist S&T Managers with determining whether a particular research topic should be developed as fundamental. If, however, in conducting the activities supported under this award, the Principal Investigator (PI) or co-PI is concerned that any portion of the research may potentially cause damage to national security and warrant Government restrictions on the dissemination of the results, the PI should promptly notify the Program Office by email.

Deemed Exports

Export control laws and requirements must be complied with when non-U.S. persons or foreign nationals are granted access to regulated products or technology by a company or institution of higher education in the United States. Under the "deemed export" rule, allowing non-U.S. persons or foreign nationals access to the product or technology may trigger the requirement to apply for a license prior to that access.

Activities Abroad

You must ensure that project activities to be performed outside the United States are coordinated as necessary with appropriate governmental authorities and that required licenses, permits, or approvals are obtained prior to undertaking such activities. The Government does not assume responsibility for your compliance with the laws and regulations of the country in which the activities are to be conducted.

Activities That Affect U.S. Persons

All work and services to be performed hereunder shall be in strict compliance with procedures set forth in DoDM 5240.01.